(19) 世界知的所有権機関 国際事務局



(43) 国際公開日 2001年10月18日(18.10.2001)

PCT

(10) 国際公開番号 WO 01/78301 A1

(51) 国際特許分類?:

H04L 9/00, G11B 20/10, 20/12

(21) 国際出願番号:

PCT/JP01/03004

(22) 国際出願日:

2001年4月6日 (06.04.2001)

(25) 国際出願の言語:

日本語

(26) 国際公開の言語:

日本語

(30) 優先権データ:

JP 特願2000-105328 2000 年4 月6 日 (06.04.2000) 2000年4月7日(07.04.2000) JP 特願2000-106039 2000年6月7日(07.06.2000) JР 特願2000-170604

特願 2000-391976

2000年12月25日(25.12.2000) JP (71) 出願人 (米国を除く全ての指定国について): ソニー株 式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および

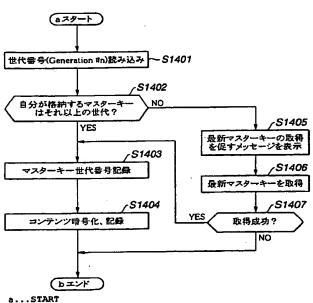
(75) 発明者/出願人 (米国についてのみ): 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo) [JP/JP]. 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 光澤 敦 (MITSUZAWA, Atsushi) [JP/JP]. 大石丈於 (OISHI, Fateo) [JP/JP]. 瀧 隆太((TAKI), Ryuta) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目 7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).

/続葉有]

(54) Title: INFORMATION RECORDING/REPRODUCING APPARATUS AND METHOD

(54) 発明の名称:情報記録/再生装置及び方法



51401...READ GENERATION NUMBER (Generation #n)

S1402...GENERATION NUMBER OF MASTER KEY THAT THE APPARATUS HAS

IS THE SAME AS OR LAGER THAN THAT READ AT \$1401

\$1403...RECORD GENERATION NUMBER OF MASTER KEY

51404...CIPHER CONTENT AND RECORD CIPHERED CONTENT

\$1405...DISPLAY MESSAGE TO PROMPT THE USER TO ACQUIRE LATEST MASTER KEY

S1406...ACQUIRE LATEST MASTER KEY

S1407...SUCCESSFUL ACQUISITION?

b...END

(57) Abstract: If the generation of a master key that a reproducing apparatus has is older than that used when data is recorded and consequently the data cannot be reproduced, or if the generation of a master key that a recording apparatus has is older than that required when data is to be recorded on a record medium and consequently the data cannot be recorded, the user is prompted to update the master key, and the user acquires a required master key to perform reproducing or recording. the updated master key is delivered in the form handled only by a specific device through a transmission medium such as a record medium, a network, an IC card, or a telephone line by using, e.g., a tree-structured key delivery system.

WO 01/78301

/毓葉有]



- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) 指定国 *(*広域*)*: ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許

(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

-- 国際調査報告書

2 文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

再生機器が持つマスターキーの世代がデータの記録時に用いられたものよりも古く再生ができない場合、及び記録機器が持つマスターキーの世代が記録媒体の記録に必要なものよりも古く記録ができない場合に、ユーザに対してマスターキーの更新を促し、必要なマスターキーを入手して再生処理又は記録処理を可能とする。更新マスターキーは、記録媒体、ネットワーク、ICカード、電話回線などの伝送媒体を用い、例えばツリー型キー配信構成を用いて、特定のデバイスにおいてのみ処理可能な形態で配信する。



明細書

情報記録/再生装置及び方法

技術分野

本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、キー更新端末装置、世代管理キー更新方法、及び情報記録媒体、並びにプログラム提供媒体に関し、特に、データ記録再生可能な記録媒体に対するデータ書き込み、データ再生処理における違法コピーを防止することを可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、キー更新端末装置、世代管理キー更新方法、及び情報記録媒体、並びにプログラム提供媒体に関する。

背景技術

ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置及び記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置及び記録媒体に違法なコピーを防止するための様々な仕組み(システム)が導入されている。

例えば、MD (ミニディスク) (MDは商標) 装置において、違法なコピーを 防止する方法として、SCMS (Serial Copy Management System) が採用されて いる。SCMSは、データ再生側において、オーディオデータとともにSCMS 信号をディジタルインタフェース (DIF) から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を 制御することにより違法なコピーを防止するシステムである。

具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー(copy free)のデータであるか、1度だけコピーが許されている(copy prohibited)データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー(copy free)となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可(copy once allowed)となっている場合には、SCMS信号をコピー禁止(copy prohibited)に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止(copy prohibited)となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行うことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランプルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

コンテンツ・スクランブルシステムでは、DVD-ROM (Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー(復号鍵)が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。したがって、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、D

VD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、ディジタルデータを記録したDVD-ROMの再生を行えないことになり、不正コピーが防止されるようになっている。

しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体(以下、適宜、ROMメディアという)を対象としており、ユーザによるデータの書き込みが可能な記録媒体(以下、適宜、RAMメディアという)への適用については考慮されていない。

すなわち、ROMメディアに記録されたデータが暗号化されていても、その暗 号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ラ イセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することがで きてしまう。

そこで、本出願人は、先の特許出願、特開平11-224461号公報(特願平10-25310号)において、個々の記録媒体を識別するための情報(以下、媒体識別情報と記述する)を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー (マスターキー) により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製 (違法コピー) ができないように、その動作が規定される。

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒

ターキーを用いてデータを暗号化して記録するようにしている。このため、古い記録媒体であっても、正当な機器によって最新に近いマスターキーを用いてデータが暗号化され記録されるため、最新のマスターキーを得られない、秘密が暴かれた機器によりこのデータが読まれるのを防ぐことができる。

上述の世代管理マスターキーを用いる構成においては、記録機器は自身が持つ 最新の世代のマスターキーを用いてデータを暗号化して記録する。その記録媒体 が別の再生機器によって再生されるためには、再生機器が記録時に使用された世 代のマスターキーを知っている必要があるが、最新世代のマスターキーは最新世 代の記録媒体にアクセスしなければ得られないため、これができていず、正当な 再生機器であっても記録されたデータを再生できないことが起こりうる。

また、記録時には、記録機器が記録媒体が許可する世代以上に新しいマスターキーを持つことが必要であるが、ある機器グループの秘密が暴かれたために、記録媒体のマスターキーテーブルからこのグループ用の暗号化マスターキーが取り除かれている可能性があり、この記録機器が正当なものであってもこの記録媒体にデータを記録できないことが起こりうる。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、不正にデータが複製されることを防止する特徴を保ったまま、インタオペラビリティをより広く確保することを可能とする情報記録装置、情報再生装置、情報記録方法、情報再生方法、キー更新端末装置、世代管理キー更新方法、及び情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

本発明の第1の側面は、記録媒体に情報を記録する情報記録装置において、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報

体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータの全てを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、*実質的に、違法コピーが防止されることになる。

しかし、先の提案におけるライセンスにより得られる秘密キー (マスターキー) は、全機器おいて共通である必要があった。これは、所定の機器で記された記録媒体を、他の機器においても再生可能とするインタオペラビリティを確保するための必要な条件であるからである。

しかし、この共通マスターキーを格納する構成であるがために、1つの機器が 攻撃者より攻撃を受け、その機器が保持していた秘密キーが暴かれてしまった場合、全ての機器の秘密キーが暴かれてしまったのと同じ結果を招くことになり、 秘密キーが暴かれる前に記録されたデータは勿論、秘密キーが暴かれた後に記録 されたデータ、その暴かれた秘密キーを用いて、解読されてしまうという課題が あった。

そこで、本件出願人は先に提案した特願平11-294928号において、上記マスターキーを世代管理する方法を提案した。すなわち、全システムで共通なマスターキーを第1世代から使用していき、機器グループ毎に固有の秘密キーを用いることにより記録媒体からその記録媒体が生産された時点の最新のマスターキーを各機器が入手できるようにした構成である。すなわち、格納キーの秘密が暴かれたグループについては、それ以降に生産される記録媒体においては次の世代のマスターキーを与えないようにしている。このようにすることで、正当な(秘密が暴かれていない)機器はより新しい世代のマスターキーを得られるが、秘密が暴かれた機器はある世代のマスターキーを最後にそれより新しいものは得られないように構成したものである。

記録機器がデータを記録媒体に記録する際には、記録媒体に格納されたマスターキーと同じ世代かより新しい世代のマスターキーを使用してのみ記録することができ、その条件に合うマスターキーを持つ記録機器は、自分が持つ最新のマス

よりも新しいものである場合に、警告出力を実行するユーザインタフェースと、 を有することを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様において、前記装置格納世代管理 暗号化キーは、複数の情報記録装置に共通に格納されたマスターキーであること を特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記装置格納世代管理暗号化キーの世代情報よりも古い世代情報の世代管理暗号化キーを、前記装置格納世代管理暗号化キーに基づいて生成するキー生成手段を有する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含み、前記更新手段は、暗号化処理の施された更新用世代管理暗号化キーについての復号処理を、前記情報記録装置に格納されたデバイスキーに基づいて実行し、更新された世代管理暗号化キーを生成する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記暗号化処理の施された更新用世代管理暗号化キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理暗号化キーについての復号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記デバイスキーは、 情報記録装置をカテゴリ区分し、共通のカテゴリに属する情報記録装置に共通の キーとした構成であることを特徴とする。

7

さらに、本発明の情報記録装置の一実施態様において、前記デバイスキーは、 情報記録装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構 成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、 複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに 固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記世代管理 暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更 新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キ

一は、複数の情報記録装置において共通なマスターキーであることを特徴とする。 さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新 可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー 更新ブロック (KRB) を更新対象となるリーフの情報記録装置に配布する構成 であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、キー更新ブロッ

ク(KRB)の暗号処理により、前記更新ノードキーを取得するとともに、該取

得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得す

る構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック (KRB) は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

さらに、本発明の第2の側面は、記録媒体に情報を記録する情報記録装置にお

いて、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得手段と、を有することを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様において、前記キー取得手段は、 ネットワークを介するデータ受信の実行可能な通信インタフェースを含むことを 特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー取得手段は、 電話回線を介するデータ受信の実行可能な通信モデムを含むことを特徴とする。 さらに、本発明の情報記録装置の一実施態様において、前記キー取得手段は、 I Cカードを介するデータ受信の実行可能な I / Cカードインタフェースを含む ことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、 前記キー取得手段によるキー取得実行の際に、キー提供手段との相互認証処理を 実行する構成を有し、前記キー取得手段は、前記相互認証処理の成立を条件とし て前記世代管理暗号化キーの取得を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記装置格納世代管理 暗号化キーは、複数の情報記録装置に共通に格納されたマスターキーであること を特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、 前記装置格納世代管理暗号化キーの世代情報よりも古い世代情報の世代管理暗号 化キーを、前記装置格納世代管理暗号化キーに基づいて生成するキー生成手段を 有する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含み、前記更新手段は、暗号化処理の施された更新用世代管理暗号化キーについての復号処理を、前記情報記録装置に格納されたデバイスキーに基づいて実行し、更新された世代管理暗号化キーを生成する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、 前記暗号化処理の施された更新用世代管理暗号化キーと、復号用のデバイスキー 識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー 一識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された 更新用世代管理暗号化キーについての復号処理を実行する構成であることを特徴 とする。

さらに、本発明の情報記録装置の一実施態様において、前記デバイスキーは、 情報記録装置をカテゴリ区分し、共通のカテゴリに属する情報記録装置に共通の キーとした構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記デバイスキーは、 情報記録装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構 成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、 複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに 固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記世代管理 暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更 新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする。 さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新 可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック (KRB) は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

さらに、本発明の第3の側面は、記録媒体に情報を記録する情報記録装置において、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーを取得するためのキー更新端末を接続するキー更新端末接続インタフェースと、を有することを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様は、前記キー更新端末からの前記 世代管理暗号化キー取得実行の際に、前記キー更新端末との相互認証処理を実行 する構成を有し、前記情報記録装置は、前記相互認証処理の成立を条件として前 記世代管理暗号化キーの取得を実行する構成である。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、 複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに 固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記世代管理 暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更 新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック (KRB) は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

さらに、本発明の第4の側面は、記録媒体から情報を再生する情報再生装置に おいて、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基 づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する 暗号処理手段と、前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、警告出力を実行するユーザインタフェースと、を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報との比較処理において前記プレ世代情報が前記記録時世代情報よりも新しいものである場合に復号処理を実行しない構成としたことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記装置格納世代管理 復号キーは、複数の情報再生装置に共通に格納されたマスターキーであることを 特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記装置格納世代管理復号キーの世代情報よりも古い世代情報の世代管理復号キーを、前記装置格納世代管理復号キーに基づいて生成するキー生成手段を有する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含み、前記更新手段は、暗号化処理の施された更新用世代管理復号キーについての復号処理を、前記情報再生装置に格納されたデバイスキーに基づいて実行し、更新された世代管理復号キーを生成する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理復号キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理復号キーについての復号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記デバイスキーは、 情報再生装置をカテゴリ区分し、共通のカテゴリに属する情報再生装置に共通の キーとした構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記デバイスキーは、 情報再生装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構 成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、 複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに 固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記世代管理 復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新 可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新プロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、キー更新プロック(KRB)の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック (KRB)は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読 み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする。

さらに、本発明の第5の側面は、記録媒体から情報を再生する情報再生装置において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処理手段と、前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得手段と、を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報との比較処理において前記プレ世代情報が前記記録時世代情報よりも新しいものである場合に復号処理を実行しない構成としたことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー取得手段は、 ネットワークを介するデータ受信の実行可能な通信インタフェースを含むことを 特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー取得手段は、 電話回線を介するデータ受信の実行可能な通信モデムを含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー取得手段は、 I Cカードを介するデータ受信の実行可能な I / Cカードインタフェースを含む ことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記キー取得手段によるキー取得実行の際に、キー提供手段との相互認証処理を 実行する構成を有し、前記キー取得手段は、前記相互認証処理の成立を条件とし て前記世代管理復号キーの取得を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記装置格納世代管理 復号キーは、複数の情報再生装置に共通に格納されたマスターキーであることを 特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、 前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しい ものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号 キーに更新処理を実行する更新手段を含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記装置格納世代管理復号キーの世代情報よりも古い世代情報の世代管理復号キーを、前記装置格納世代管理復号キーに基づいて生成するキー生成手段を有する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含み、前記更新手段は、暗号化処理の施された更新用世代管理復号キーについての復号処理を、前記情報再生装置に格納されたデバイスキーに基づいて実行し、更新された世代管理復号キーを生成する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記暗号化処理の施された更新用世代管理復号キーと、暗号復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理復号キーについての復号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記デバイスキーは、 情報再生装置をカテゴリ区分し、共通のカテゴリに属する情報再生装置に共通の キーとした構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記デバイスキーは、 情報再生装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構 成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、 複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに 固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記世代管理 復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新 可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック (KRB) は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使

用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする。

さらに、本発明の第6の側面は、記録媒体から情報を再生する情報再生装置において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処理手段と、前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーを取得するためのキー更新端末を接続するキー更新端末接続インタフェースと、を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新端末からの前記世代管理復号キー取得実行の際に、前記キー更新端末との相互認証処理を 実行する構成を有し、前記情報再生装置は、前記相互認証処理の成立を条件として前記世代管理復号キーの取得を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、 複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに 固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記世代管理 復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新 可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで

暗号化処理した前記世代管理復号キーの更新データを受領し、キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック (KRB) は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする。

さらに、本発明の第7の側面は、記録媒体に情報を記録する情報記録方法において、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、さらに、情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、警告出力を実行する警告出力ステップと、を有することを特徴とする情報記録方法にある。

さらに、本発明の第8の側面は、記録媒体に情報を記録する情報記録方法において、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、さらに、情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世

代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得ステップと、を有することを特徴とする情報記録方法にある。

さらに、本発明の情報記録方法において、前記キー取得ステップは、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて前記世代管理暗号化キーの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された世代管理暗号化キーに基づいて前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を含むことを特徴とする。

さらに、本発明の情報記録方法において、前記世代管理暗号化キーは、複数の 情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報記録方法において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報記録装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

さらに、本発明の情報記録方法において、前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、さらに、前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

さらに、本発明の第9の側面は、記録媒体から情報を再生する情報再生方法において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体の格納情報の復号処理を実行する復号処理ステップを有し、さらに、情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、前記記録時世代情報が、前記

装置格納世代管理復号キーの世代情報よりも新しいものである場合に、警告出力 を実行する警告出力ステップと、を有することを特徴とする情報再生方法にある。

さらに、本発明の第10の側面は、記録媒体から情報を再生する情報再生方法において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体の格納情報の復号処理を実行する復号処理ステップを有し、さらに、情報記録再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得ステップと、を有することを特徴とする情報再生方法にある。

さらに、本発明の情報再生方法において、前記キー取得ステップは、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する世代管理復号キーの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された世代管理復号キーに基づいて前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を含むことを特徴とする。

さらに、本発明の情報再生方法において、前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生方法において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

さらに、本発明の情報再生方法において、前記世代管理復号キーは、更新情報

としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して実行することを特徴とする。

さらに、本発明の第11の側面は、情報の記録可能な情報記録媒体であって、 該情報記録媒体に対する暗号化データの書き込みに使用可能な暗号化キー、又は 該情報記録媒体の格納データの復号処理に使用可能な復号キーとして許容される キーの世代情報としてのプレ世代情報を格納したことを特徴とする情報記録媒体 にある。

さらに、本発明の情報記録媒体の一実施態様において、前記プレ世代情報は、 前記情報記録媒体における書き換え不可領域に記録されていることを特徴とする。

さらに、本発明の第12の側面は、世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行うキー更新端末装置であり、前記情報記録又は再生装置に接続可能なインタフェースと、外部との通信を実行する通信手段と、前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理、該装置固有識別子の前記通信手段を介する送信処理、前記通信手段を介する更新世代管理キーの受信処理、及び前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理の各制御を実行する制御手段と、を有することを特徴とするキー更新端末装置にある。

さらに、本発明の第13の側面は、世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行うキー更新端末装置であり、前記情報記録又は再生装置に接続可能なインタフェースと、装置固有の暗号化鍵で暗号化された世代管理キーを、前記情報記録又は再生装置の装置固有識別子に対応付けたキーテーブルを格納した記憶手段と、前記インタフェース

を介する前記情報記録又は再生装置からの装置固有識別子の取得処理、該装置固有識別子に基づく前記記憶手段からの該装置固有識別子に対応する暗号化世代管理キーの取得処理、及び前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理の各制御を実行する制御手段と、を有することを特徴とするキー更新端末装置にある。

さらに、本発明のキー更新端末装置の一実施態様において、前記情報記録又は 再生装置との相互認証処理を実行する構成を有し、前記キー更新端末装置は、前 記相互認証処理の成立を条件として前記世代管理キーの前記情報記録又は再生装 置に対する提供処理を実行する構成であることを特徴とする。

さらに、本発明の第14の側面は、世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行う世代管理キー更新方法であり、前記情報記録又は再生装置に接続可能なインタフェースと、外部との通信を実行する通信手段とを有するキー更新端末装置を前記情報記録又は再生装置に接続するステップと、前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理ステップと、装置固有識別子の前記通信手段を介する送信処理ステップと、前記通信手段を介する更新世代管理キーの受信処理ステップと、前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理ステップと、を有することを特徴とする世代管理キー更新方法にある。

さらに、本発明の第15の側面は、世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行う世代管理キー更新方法であり、前記情報記録又は再生装置に接続可能なインタフェースと、装置固有の暗号化鍵で暗号化された世代管理キーを、前記情報記録又は再生装置の装置有識別子に対応付けたキーテーブルを格納した記憶手段とを有するキー更新端末装置を前記情報記録又は再生装置に接続するステップと、前記インタフェー

スを介する前記情報記録又は再生装置からの装置固有識別子の取得処理ステップと、装置固有識別子に基づく前記記憶手段からの該装置固有識別子に対応する暗号化世代管理キーの取得処理ステップと、前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理ステップと、を有することを特徴とする世代管理キー更新方法にある。

さらに、本発明の世代管理キー更新方法において、前記情報記録又は再生装置 との相互認証処理を実行するステップを有し、前記相互認証処理の成立を条件と して前記世代管理キーの前記情報記録又は再生装置に対する提供処理を実行する ことを特徴とする。

さらに、本発明の第16の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、さらに、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、警告出力ステップ、あるいは前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得ステップと、の少なくともいずれかを実行するステップを有することを特徴とするプログラム提供媒体にある。

さらに、本発明のプログラム提供媒体の一実施態様において、前記コンピュータ・プログラムは、さらに、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する世代管理暗号化キーの更新処理を実行する更新ステップを含むことを特徴とする。

さらに、本発明の第17の側面は、記録媒体から情報を再生する情報再生処理 をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供す るプログラム提供媒体であって、前記コンピュータ・プログラムは、情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体からの格納情報の復号処理を実行する復号処理ステップを有し、さらに、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、警告出力ステップ、あるいは前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得ステップと、の少なくともいずれかを実行するステップを有することを特徴とするプログラム提供媒体にある。

さらに、本発明のプログラム提供媒体の一実施態様において、前記コンピュータ・プログラムは、さらに、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する世代管理復号キーの更新処理を実行する更新ステップを含むことを特徴とする。

本発明においては、再生機器が持つマスターキーの世代がデータの記録時に用いられたものよりも古く再生ができない場合に、ユーザに対してマスターキーの 更新を促し、必要なマスターキーを入手して再生処理を可能とする。マスターキーの入手は、データを記録する記録媒体以外の媒体、あるいはネットワークなど の伝送媒体を用いて行って、入手したマスターキーを用いて再生処理を行う。

また、本発明においては、記録機器が持つマスターキーの世代が記録媒体の記録に必要なものよりも古く記録ができない場合に、ユーザに対してマスターキーの更新を促し、必要なマスターキーを入手して記録処理を可能とする。マスターキーの入手は、データを記録する記録媒体以外の媒体、あるいはネットワークなどの伝送媒体を用いて行って、入手したマスターキーを用いて記録処理を行う。

なお、本発明の第16及び第17の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒

体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

٠.

- 図1は、本発明の情報記録再生装置の暗号処理部構成を示すプロック図である。
- 図2は、本発明の情報記録再生装置のマスターキー管理構成を示す図である。
- 図3は、本発明の情報記録再生装置のマスターキー更新処理フローを示す図である。
- 図4は、本発明の情報記録再生装置のマスターキー更新処理を示すブロック図である。
 - 図5は、本発明の情報記録再生装置の情報再生処理フローを示す図である。
 - 図6は、本発明の情報記録再生装置(例1)の構成を示すブロック図である。
- 図7は、本発明の情報記録再生装置において厳格なマスターキー世代管理を可能とした暗号処理部構成を示すブロック図である。
- 図8は、厳格なマスターキー世代管理を可能とした情報記録再生装置におけるマスターキー管理構成を示す図である。
- 図9は、厳格なマスターキー世代管理を可能とした情報記録再生装置における コンテンツ記録処理フローを示す図である。
 - 図10は、厳格なマスターキー世代管理を可能とした情報記録再生装置におけ

るマスターキー更新処理フローを示す図である。

- 図11は、マスターキー世代管理を可能とした情報記録再生装置におけるマスターキー世代情報格納構成を示す図である。
- 図12は、厳格なマスターキー世代管理を可能とした情報記録再生装置におけるコンテンツ再生処理フローを示す図である。
 - 図13は、本発明の情報記録再生装置 (例2) の構成を示すプロック図である。
 - 図14は、厳格なマスターキー世代管理を可能とした情報記録再生装置(例
- 2) におけるコンテンツ記録処理フローを示す図である。
- 図15は、厳格なマスターキー世代管理を可能とした情報記録再生装置 (例
- 2) におけるコンテンツ再生処理フローを示す図である。
 - 図16は、本発明の情報記録再生装置 (例3) の構成を示すブロック図である。
- 図17は、厳格なマスターキー世代管理を可能とした情報記録再生装置(例
- 3)におけるコンテンツ記録処理フローを示す図である。
- 図18は、本発明の情報記録再生装置におけるキー取得処理に適用可能な認証 処理(共通鍵方式)の処理シーケンスを示す図である。
- 図19は、本発明の情報記録再生装置におけるキー取得処理に適用可能な認証 処理(公開鍵方式)の処理シーケンスを示す図である。
- 図20は、本発明の情報記録再生装置におけるキー取得処理に適用可能な認証 処理に用いられる公開鍵証明書の構成を示す図である。
- 図21は、本発明の情報記録再生装置におけるリポケーションリストの構成を 示す図である。
- 図22は、本発明の情報記録再生装置におけるレジストレーションリストの構成を示す図である。
- 図23は、本発明の情報記録再生装置におけるコンテンツ再生処理フローを示す図である。
- 図24は、本発明の情報記録再生装置において使用されるキー更新端末の構成 を示すブロック図である。
- 図25は、本発明の情報記録再生装置におけるキー更新端末を使用したキー更新処理を説明するブロック図(その1)である。

- 図26は、本発明の情報記録再生装置におけるキー更新端末を使用したキー取得処理に適用可能な認証処理(共通鍵方式)の処理シーケンスを示す図である。
- 図27は、本発明の情報記録再生装置におけるキー更新端末を使用したキー取 得処理に適用可能な認証処理(公開鍵方式)の処理シーケンスを示す図である。
- 図28は、本発明の情報記録再生装置におけるキー更新端末を使用したキー取得処理においてキー発行機関が有するキーテーブルの例を示す図である。
- 図29は、本発明の情報記録再生装置におけるキー更新端末を使用したキー更新処理を説明するブロック図(その2)である。
- 図30は、本発明の情報記録再生装置におけるキー更新端末を使用したキー更新処理を説明するブロック図(その3)である。
- 図31は、本発明の情報記録再生装置におけるキー更新端末を使用したキー更新処理を説明するブロック図(その4)である。
- 図32は、本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。
- 図33A及び図33Bは、本発明の情報記録再生装置に対するマスターキー、 メディアキー等の鍵の配布に使用されるキー更新ブロック (KRB) の例を示す 図である。
- 図34は、本発明の情報記録再生装置におけるマスターキーのキー更新ブロック (KRB) を使用した配布例と復号処理例を示す図である。
- 図35は、本発明の情報記録再生装置におけるマスターキーのキー更新プロック (KRB) を使用した復号処理フローを示す図である。
- 図36は、本発明の情報記録再生装置において、外部からKRBを通信手段等を介して受信し、記録媒体に格納する処理について示すブロック図である。
- 図37は、本発明の情報記録再生装置において、外部からKRBを通信手段等を介して受信し、記録媒体に格納する処理フローを示す図である。
- 図38は、本発明の情報記録再生装置において、外部からKRBを通信手段等を介して受信し、記録媒体に格納する処理を説明する図である。
 - 図39は、本発明のシステムにおいて利用可能な記録媒体の例を示す図である。
 - 図40は、本発明の情報記録再生装置において、データ処理をソフトウェアに

よって実行する場合の処理手段構成を示したブロック図である。

発明を実施するための最良の形態

[1.マスターキー世代管理の基本構成]

図1は本発明の情報再生装置100における暗号処理部の処理機能を中心とした一実施形態の構成を示すブロック図である。情報再生装置のデバイスキー保持部101は、この情報再生装置100に与えられたデバイスキーD K_j を保持している。暗号文保持部102は、暗号化マスターキーC(j,i)(デバイスキーDKで暗号化されたマスターキー MK_i)を保持している。このような、デバイスキーD K_j 、マスターキー MK_i 、及び暗号化マスターキーC(j,i) の関係を、C(j,i) = $Enc(DK_j,MK_i)$ と表す。

なお、iはマスターキーの世代番号を表し、jは、カテゴリ番号を表す。このカテゴリ番号とは、情報再生装置などのデバイスに対して割り当てられた番号であり、1台のデバイス毎、またデバイスのメーカー毎、又はデバイスのモデル毎、又はデバイスのロット毎、又は予め定められた数のデバイス、例えばデバイスに付与されたシリアルナンバの所定単位毎などに割り振られている。以下、デバイスキーDK_jを、カテゴリ番号jを用いて区別する必要がない場合、単にデバイスキーDKと記述し、同様にマスターキーMKも、世代番号iを用いて区別する必要がない場合、単にマスターキーMKも、世代番号iを用いて区別する必要がない場合、単にマスターキーMKと記述する。これらに対応して、暗号化マスターキーC(j, i) も、単に暗号化マスターキーCと記述する。

デバイスキーDKと暗号化マスターキーCは、デバイスに対してキーを発行するキー発行機関から与えられ、予め記憶されている。キー発行機関は、マスターキーMKを保管するとともに、デバイスキーDKをカテゴリ番号jに対応付けて秘密裡に保管する。

マスターキー復号部103は、デバイスキー保持部101で保持されているデパイスキーDKを用いて、暗号文保持部102で記憶されている暗号化マスターキーCを復号し、マスターキーMKを得る。すなわち、暗号文Xを、キーYで復号する関数をDEC(Y,X)と表すと、マスターキー復号部103では、式MK i=

DEC (DK_j, C(j,i)) が演算される。得られたマスターキーMKは、解読部104に供給される。

解読部104は、データ読み出し部105により、記録媒体(光ディスク)150などから読み出された、マスターキーMKに基づいて暗号化されているデータを、マスターキー復号部103から供給されたマスターキーMKを用いて解読する。すなわち、記録媒体(光ディスク)150には、マスターキーMKに基づいて暗号化されたデータが記録されており、解読部104は、この暗号化されたデータを、マスターキーMKについて解読(復号)する。解読されたデータが、例えば、画像データである場合、表示デバイスに出力され、表示される。また、データ読み出し部105は、後述する処理によりマスターキーMKを更新する場合、更新用のデータが記録された記録媒体(光ディスク)150から、マスターキーMKを、デバイスキーDKに基づいて暗号化した暗号化マスターキーCを読み出し、暗号文保持部102に出力する。

次に、情報再生装置のマスターキーMKの更新について説明する。マスターキーMKの更新は、世代iのマスターキーMK_iが、攻撃者などにより暴かれてしまった場合等の不定期に、あるいは所定同期で定期的に行われる。以下の説明では、マスターキー_iの更新のため、全てのデバイスのデバイスキーDK_jで暗号化されたマスターキーMK_i(暗号化マスターキーC(j,i))が記録された光ディスクが、キー発行機関から配布されるものとする。なお、勿論、暗号化マスターキーC(j,i)は、光ディスク以外の記録媒体や、インターネットなどネットワークを用いて配布してもよい。また、記録媒体(光ディスク)150は、マスターキーMK_iの更新専用のものである必要はなく、ビデオデータやオーディオデータ等のコンテンツが記録されたもの、あるいはコンテンツの記録が、これから可能なものであってもよい。

図 2 に、記録媒体(光ディスク) 1 5 0 に記録されている暗号化マスターキー C (j,i) の例を示す。この例は、世代i のマスターキーM K_i を世代i + 1 のマスターキーM K_i + 1 に更新する場合の例である。すなわち、光ディスク 1 5 0 には、カテゴリ番号 j と、マスターキーM K_i + 1 を、カテゴリ番号 j のデバイスキーD K_i j に基づいて暗号化した暗号化マスターキーC (j, i + 1) とが、そ

れぞれ対応付けられて記録されている。

図2に示したように、全てのカテゴリ番号jにおいて、マスターキーMK_i+1 は共通とされている。このように、各デバイスのマスターキーMKを共通にすることにより、ライセンスを受け、正式なデバイスキーDKを保持するデバイス間では、マスターキーMKにより暗号化されたデータを共用すること、即ち、インタオペラビリティを保つことが可能となる。また、正式なデバイスキーDKを保持しないデバイスは、マスターキーMKを復号することができないので、そのマスターキーMKで暗号化されたデータを復号することは不可能となる。

例えば、カテゴリ番号 2 のデバイスが、攻撃者から攻撃を受け、そのデバイスキーD K_2 が暴かれてしまったことがわかっている場合、図 2 に示したように、マスターキーM K の更新用のデータ(暗号化マスターキーC(j, i+1))のうちの、カテゴリ番号 2 に対応する暗号化マスターキーC(2, i+1)の欄は空欄とされる。このようにして、デバイスキーD K が暴かれてしまったデバイスには、新たな世代のマスターキーM K_i 1+1 を付与しないことにより、デバイスキーD K_2 を持つデバイスを正当な利用権を有するグループからリポーク(排除)することができる。

図3のフローチャートを参照して、世代iのマスターキーMK_iを世代i+1のマスターキーMK_i+1に更新する際の情報再生装置の動作について説明する。ステップS301において、上述したようなマスターキーMKの更新用のデータが記録された記録媒体(光ディスク)150が、ユーザにより情報再生装置にセットされる。情報再生装置のデータ読み出し部105は、ステップS302において、セットされた光ディスクから、自分のカテゴリ番号j(記憶しているデバイスキーDK)に割り当てられている暗号化マスターキーC(j,i+1)を読み出す。例えば、カテゴリ番号jが3である場合、暗号化マスターキーC(3,i+1)が読み出される。

このようにして読み出された暗号化マスターキーC (j, i+1) は、ステップ S 3 0 3 において、暗号文保持部 1 0 2 に記憶される。暗号文保持部 1 0 2 には、このようにして更新された暗号化マスターキーC (j, i+1) のみが記憶される。

以上のようにして、暗号文保持部102に記憶された暗号化マスターキーC (j, i+1) を用いて、光ディスク150に記録されているマスターキーMK に基づいて暗号化されたデータを再生する場合には、図4に示すように、マスターキー復号部103は、デバイスキー保持部101に保持されているデバイスキー:DK_jに基づいて、暗号文保持部102に記憶されている暗号化マスターキーC (j, i+1) を復号することにより、マスターキーMK_i+1を得る。そして、このマスターキーMK_i+1に基づいて、記録媒体(光ディスク)150に記録されている暗号化されたデータが復号される。

このデータ再生処理手順を図5のフローチャートに示す。まず最初に、ステップS5001において、情報再生装置のデータ読み出し部105は、セットされている記録媒体(光ディスク)150からデータを読み出す。ここで、記録媒体(光ディスク)150は、リードインエリアとデータエリアから構成されており、リードインエリアには、データエリアに記録されているデータのファイル名やディレクトリ情報などのTOC(Table Of Contents)などが記録されている。また、リードインエリアには、データエリアのデータがどの世代のマスターキーMKを用いて暗号化されているのかを示すデータ(世代情報)も記録されている。なお、この世代情報は、データを記録するときの暗号化に用いられたマスターキーMKの世代を表すので、以下、適宜、記録時世代情報という。

ステップS501では、データ読み出し部105において、リードインエリアのデータが読み出され、ステップS502に進む。ステップS502において、マスターキー復号部103は、暗号文保持部102を介して供給される、データ読み出し部105が読み出したデータから、データエリアのデータを暗号化するのに用いられたマスターキーMKの世代iを調べる。そして、ステップS503に進み、マスターキー復号部103は、調べたマスターキーMKの世代iのマスターキーMK iを作成する。

例えば、調べたマスターキーMKの世代が、最新世代の世代i+1である場合、マスターキー復号部103は、デバイスキー保持部101に保持されているデバイスキーDKを用いて、暗号文保持部102に記憶されている暗号化マスターキーC(j, i+1)を復号することにより、マスターキーMK_i+1を作成する。

また、調べたマスターキーM K の世代が、暗号文保持部 1 0 2 に保持されている以前の世代である場合、マスターキー復号部 1 0 3 は、暗号文保持部 1 0 2 に記憶されている暗号化マスターキーCから、その世代のマスターキーM K を作成する。すなわち、マスターキー復号部 1 0 3 は、まず、上述したようにしてマスターキーM K 上述したようにしてマスターキーM K の世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーM K を作成する。

例えば、暗号文保持部 102 に記憶されているマスターキーM K の世代が世代 i+1であり、読み取られたマスターキーM K の世代が世代 i-1である場合、マスターキーM K $_1-1$ は、マスターキー復号部 103 において、一方向性関数 f が $_2$ 回用いられ、 f (f (M K $_1+1$)) が計算されることにより生成される。また、暗号文保持部 102 に記憶されているマスターキーM K の世代が世代 i+1であり、読み取られたマスターキーM K の世代が世代 i-2である場合、マスターキーM K $_1-2$ は、一方向性関数 f を $_2$ 回用いて、 f (f (f (M K $_1-1+1$)) が計算されることにより生成される。

ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、MD 5 (Message Digest 5)や、SHA-1 (Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキー MK_1 , MK_2 , \cdots , MK_n , NE, NE,

また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘

密鍵に対する公開鍵を、全ての情報再生装置に与えておく。そして、キー発行機関は、第1世代のマスターキーMK_1を設定し、そのマスターキーMK_1から使用していく。すなわち、キー発行機関は、第2世代以降のマスターキーMK_iが必要になったら、その1世前のマスターキーMK_i-1を、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、N世代のマスターキーを、予め生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。

なお、情報再生装置では、ある世代のマスターキーMKを有していれば、そのマスターキーMKを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

以上のように、マスターキー復号部103は、最新世代のマスターキーMKの暗号化マスターキーCを用いて、その世代より前の世代のマスターキーMKを作成できるので、暗号文保持部102は、最新世代のマスターキーMKの暗号化マスターキーCのみを記憶していればよい。

ステップS503において、調べた世代のマスターキーMKが作成(復号)されたら、ステップS504において、データ読み出し部105は、記録媒体(光ディスク)150のデータエリアからデータを読み出す。さらに、ステップS504において、解読部104は、ステップS503で得られたマスターキーMKを用いて、データ読み出し部105が読み出したデータを解読(復号)する。解読されたデータは、例えば、そのデータが画像データである場合、ステップS505において、表示デバイスに出力され、表示される。

以上のように、自身の世代より前の世代を生成可能なマスターキーMKを、各デバイスが保持しているデバイスキーDKにより暗号化して配布することで、マスターキーMKを更新するようにしたので、インタオペラビリティを保ったまま、マスターキーMKを更新したり、暴かれたデバイスキーDKを保持するデバイスを排除することが可能となる。また、各デバイスは、一方向性関数 f を用いることにより、最新世代のマスターキーMKを保持していれば、指定のマスターキーMKを作成できるので、デバイスが所持しなくてはならないメモリの容量を削減することが可能となる。

ここで、情報再生装置においては、データの復号に用いられたマスターキーM Kは、その復号の終了後に廃棄される。そして、マスターキーM Kは、再び必要 となったときに、暗号化マスターキーCを、デバイスキーD Kに基づいて復号することで生成される。情報再生装置では、このようにして、暗号化されていないマスターキーM K が放置されることによる秘匿性の劣化が防止されるようになっている。

さらに、上述の場合においては、暗号文保持部102に、更新後の世代の暗号 化マスターキーCのみを記憶させるようにしたが、暗号文保持部102には、そ の他、各世代の暗号化マスターキーCを記憶させるようにしてもよい。この場合、 各世代のマスターキーMKを計算せずに済み、その分の処理負担が軽減される。

なお、上述のように、一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーMK_1, MK_2, ・・・, MK_Nについては、その逆に、自身の世代より後の世代を生成することはできないから、古い世代のマスターキーMKから、新しい世代のマスターキーMKが生成されることによって、データが不正に復号されることはない。

ところで、上述した構成においては、マスターキーMKを更新することで、その更新後のマスターキーMKに基づいて暗号化されたデータは保護することが可能となるが、更新前のマスターキーMKに基づいて暗号化されたデータの保護には、やや課題が残る。すなわち、上述のようなマスターキーの更新処理方法は、データを、マスターキーで暗号化して記録する記録装置にも適用可能であり、記録装置において、前の世代のマスターキーMKが用いられた暗号化がなされてしまうと、上述のように、攻撃者から攻撃を受け、新たな世代のマスターキーMKが与えられない情報再生装置(即ちリボークされるべきデバイス)であっても、その前の世代のマスターキーMKを有していれば、記録媒体からの再生が可能となる。

したがって、前の世代のマスターキーMKを用いて暗号化処理を行っている記録装置、即ち、マスターキーMKを更新しない、あるいはできない記録装置が長時間使用されると、その間に、不正な情報再生装置、即ち、新たな世代のマスターキーMKが与えられない情報再生装置によって、データが復号されてしまうこ

とになる。

- [2. 厳格なマスターキー世代管理を可能とした構成]
- (2.1.記録再生装置構成)

上述の問題を解決する構成を備えた記録再生装置600の一実施形態の構成例を図6に示す。バス610は、ディジタルI/F(Interface)620,MPEG (Moving Picture Experts Group)コーデック630、例えば暗号化/復号LSI (Large Scale Integrated Curcuit)によって構成される暗号処理手段650、C PU(Central Processing Unit)670、メモリ680、記録媒体I/F690、及びユーザI/F660を相互に接続している。

A/D, D/A コンパータ 6 3 5 は、MPEG コーデック 6 3 0 からのMPEG G デコードされたディジタル信号を、D/A (Digital Analog)変換することで、アナログ信号とし、アナログ I/F 6 4 0 に供給するとともに、アナログ I/F 6 4 0 からのアナログ信号を、A/D (Analog Digital)変換することで、ディジタル信号とし、MPEG コーデック 6 3 0 に出力する。アナログ I/F 3 5 は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D, D/A コンパータ 6 3 5 に出力するとともに、A/D, D/A コンパータ 6 3 5 からのアナログ信号を、外部に出力するようになっている。

暗号処理手段650は、例えば、1チップのLSI(Large Scale Integrated Curcuit)で構成され、バス610を介して供給されるコンテンツとしてのディジタル信号を暗号化し、又は復号し、バス610上に出力する構成を持つ。なお、暗号処理手段650は1チップLSIに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構

成による処理手段としての構成については後段で説明する。

CPU670は、メモリ680に記憶されたプログラムを実行することで、MPEGコーデック630や暗号処理手段650等を制御するとともに、各種の処理を行う。メモリ680は、例えば、不揮発性メモリで、CPU670が実行するプログラムや、CPU670の動作上必要なデータを記憶する。記録媒体I/F690は、例えば、光ディスク等の記録媒体200からディジタルデータを読み出し(再生し)、バス610上に出力するとともに、バス610を介して供給されるディジタルデータを、記録媒体200に供給して記録する構成となっている。

ユーザI/F660は、図示しない表示部や入力部を備え、ユーザに情報を提示したりユーザからの指示を受け取ってバス610に出力したりする。

(2.2. 暗号処理部構成)

次に、図7を用いて、図6に示す暗号処理手段650(ex.暗号化/復号LSI)の詳細構成について説明する。なお、図中、図1の情報再生装置における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

エンコーダ701は、マスターキー復号部103が出力するマスターキーMKに基づいて、バス610を介して供給される平文のコンテンツ(平文コンテンツ)を暗号化することにより暗号文(暗号化コンテンツ)とし、その暗号化コンテンツを、バス610上に出力する。デコーダ702は、マスターキー復号部103が出力するマスターキーMKに基づいて、バス610を介して供給される暗号化コンテンツを復号することにより平文コンテンツとし、その平文コンテンツを、バス610上に出力する。マスターキー更新部703は、暗号文保持部102に記憶されたマスターキーMKの更新を制御する。

(2. 3. キーテーブル・フォーマット)

次に、図6の記録再生装置600が、記録再生の対象とする記録媒体200のフォーマットの例を図8に示す。図8に示す実施形態は、図2における記録媒体(光ディスク)150と同様の、世代iのマスターキーMK_iを、世代i+1のマスターキーMK_i+1に更新するキーテーブルを格納した記録媒体200を示し

ており、記録媒体 200には、上述の光ディスク 150における場合と同様の、カテゴリ番号 j と暗号化マスターキーC (j, i+1) とが、それぞれ対応付けられたテーブル(キーテーブル)が記録されている。さらに、記録媒体 200には、この記録媒体 200に対するデータの記録及び再生に必要なマスターキーM Kの最小の世代を表す世代情報Generation#nが記録されている。ここで、この世代情報Generation#nは、例えば、記録媒体 200の製造時に、予め記録されるものであり、上述の記録時世代情報と区別するために、以下、適宜、プレ記録世代情報 (Pre Recording Generation#n) という。

この図8に示す記録媒体200に対するデータの記録及び再生に必要なマスターキーMKの最小の世代は世代番号:nである。世代番号:nは例えばシーケンシャルな世代番号として付与される。記録再生装置600が自身の記憶手段に格納しているマスターキーの世代がnより以前である場合は、図8に示す記録媒体200に対する記録、及び記録媒体200からの再生が拒否される。

図8に示す記録媒体200は、各記録再生装置に格納したデバイスキーDKによってキーテーブルに格納された暗号化マスターキーC(i+1)を復号処理することによってマスターキーMK_i+1を取得可能とした記録媒体である。

なお、キーテーブルは全ての記録媒体に格納されるものではなく、単に世代番号 (ブレ記録世代番号) のみが記録された記録媒体200を記録再生装置600 に装着して記録あるいは再生を実行する場合には、世代番号 (ブレ記録世代番号) と各記録再生装置に格納されたマスターキーの世代番号の比較処理が記録再生装置600において実行され、記録再生装置600が自身の記憶手段の格納マスターキーの世代が記録媒体の世代番号 (ブレ記録世代番号) nより古いものである場合は、図8に示す記録媒体200に対する記録、及び記録媒体200からの再生が行えない。

図8に示す記録媒体200に対するデータの記録及び再生に必要なマスターキーMKの最小の世代はnである。記録再生装置600が自身の記憶手段に格納しているマスターキーの世代がnと同一か、より新しい記録再生装置は、記録媒体200への記録が行える。しかし、記録再生装置600が自身の記憶手段に格納しているマスターキーの世代がnより古い場合には、記録媒体200へのデータ

の記録は許されず、たとえ不正装置が古いマスターキーを用いて記録を行ったとしても、正しい再生装置はこのデータを再生しない。また、記録媒体200に正当に記録されるデータは必ずれと同一かより新しい世代のマスターキーに基づいて暗号化されて記録されるため、記録再生装置600が自身の記憶手段に格納しているマスターキーの世代がれより古い場合には、この記録再生装置は記録媒体のデータを復号できない(再生できない)ことになる。

なお、キーテーブル及びプレ記録世代情報Generation finは、記録媒体200において、その書き換えが不可能な領域(書き換え不可の領域)としての、例えば、リードインエリアに記録されており、これにより、キーテーブル及びプレ記録世代情報Generation finが不正に書き換えられることを防止するようになっている。

図8に示す記録媒体200に対するデータの記録は、その記録媒体200におけるプレ記録世代情報が表す世代以後の世代のマスターキーMKを有していなければ行うことができない(許可されない)ように、装置の設計を行う。したがって、ある世代れを表すプレ記録世代情報Generation#nが記録された記録媒体200が流通することで、記録媒体200に対する記録を行う記録装置や、その記録再生が可能な図6の記録再生装置におけるマスターキーの更新が促進され、これにより、前の世代のマスターキーMKを用いている記録装置や記録再生装置が減少していき、その結果、不正なデータの復号が防止される。

すなわち、プレ記録世代情報が記録されていない、例えば前述の図4を用いて説明した記録媒体(光ディスク)150に対しては、上述のように、マスターキーを更新していない記録装置によって、データの記録が可能であり、そのようにしてデータが記録された光ディスク150は、マスターキーを更新していない情報再生装置で再生することができてしまうが、一方、プレ記録世代情報が記録されている図8を用いて説明した記録媒体200に対しては、プレ記録世代情報が表す世代以後の世代のマスターキーMKを有していなければ、データの記録が許可されない。すなわち、記録媒体200へのデータの記録を行うには、そこに記録されているプレ記録世代情報が表す世代以後の世代のマスターキーMKが必要となるから、マスターキーを更新していない記録装置によるデータの記録が防止される。

なお、本実施の形態では、記録媒体200に記録されているキーテーブルにおけるマスターキーの世代が、プレ記録世代情報Generation#nとして記録されているものとする。但し、記録媒体200に記録されているキーテーブルにおけるマスターキーの世代と、プレ記録世代情報Generation#nが表す世代nとは、必ずしも一致している必要はない。

(2.4.マスターキー更新処理)

次に、図9乃至12を参照して、図6の記録再生装置の各種処理について説明する。まず最初に、図9のフローチャートを参照して、データの記録又は再生のために、記録媒体200が、記録再生装置にセットされたとき等に行われるマスターキー更新処理について説明する。

記録媒体 200が、記録再生装置にセットされると、まず最初に、ステップS 901において、記録媒体 I/F690 (図6参照) は、記録媒体 200から、キーテーブル世代情報Generation#i+1を読み出し、暗号処理手段 650のマスターキー更新部 703 (図7参照) に供給する。マスターキー更新部 703 は、暗号文保持部 102 が記憶している暗号化マスターキー C を読み出し、ステップ S902において、その暗号化マスターキーの世代と、キーテーブル世代情報 C Generation#i+1が表す世代i+1とを比較して、その世代の前後を判定する。

ステップS 9 0 2 において、キーテーブル世代情報Generation#i+1が表す世代i+1の方が、暗号文保持部102に記憶された暗号化マスターキーCの世代よりも後でない(新しくない)と判定された場合、即ち、暗号文保持部102に記憶された暗号化マスターキーCの世代が、キーテーブル世代情報Generation#i+1が表す世代i+1と同一か、又は後の場合、ステップS 9 0 3 乃至S 9 0 5 をスキップして、マスターキー更新処理を終了する。

すなわち、この場合、暗号文保持部102に記憶されたマスターキーMK (暗号化マスターキーC)の更新は行う必要がないので、その更新は行われない。

一方、ステップS902において、キーテーブル世代情報Generation#i+1が表す世代i+1の方が、暗号文保持部102に記憶された暗号化マスターキーCの世代よりも後である(新しい)と判定された場合、即ち、暗号文保持部102に記憶された暗号化マスターキーCの世代が、キーテーブル世代情報Generation

#i+1が表す世代i+1よりも前の世代である場合、ステップS903に進み、記録媒体I/F690は、記録媒体200(図8参照)から、キーテーブルを読み出し、暗号処理手段650(図7参照)のマスターキー更新部703に供給する。

マスターキー更新部703では、ステップS904において、キーテーブル、 自身のデバイス番号」に割り当てられた暗号化マスターキーCが存在するかどう かが判定され、存在しないと判定された場合、ステップS905をスキップして、 マスターキー更新処理を終了する。

すなわち、例えば、図2を参照して説明したように、記録再生装置が、攻撃者から攻撃を受け、そのデバイスキー DK_j が暴かれてしまったことがわかっている場合には、キーテーブルにおけるカテゴリ番号jに対応する暗号化マスターキーC(j, i+1)の欄は空欄とされるため、マスターキーMKの更新は行われない(行うことができない)。

一方、ステップS 9 0 4 において、キーテーブルに、自身のデバイス番号jに 割り当てられた暗号化マスターキーCが存在すると判定された場合、ステップS 9 0 5 に進み、マスターキー更新部 7 0 3 は、その暗号化マスターキーCを、暗 号文保持部 1 0 2 に供給し、そこに記憶されている暗号化マスターキーに替えて 記憶させ、マスターキー更新処理を終了する。

(2.5. コンテンツ記録処理)

次に、図10のフローチャートを参照して、記録媒体200に対してデータの 記録が行われる場合の、記録再生装置の処理について説明する。

まず最初に、ステップS1001において、記録媒体 I / F690は、記録媒体200から、プレ記録世代情報Generation#nを読み出し、CPU670に供給する。CPU670は、暗号処理手段650(図7)の暗号文保持部102が記憶している暗号化マスターキーCの世代を認識し、ステップS1002において、その暗号化マスターキーの世代と、プレ記録世代情報Generation#nが表す世代 n とを比較して、その世代の前後を判定する。

ステップS1002において、暗号文保持部102に記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代n以後でないと判

定された場合、即ち、暗号文保持部102に記憶された暗号化マスターキーCの 世代が、プレ記録世代情報Generation#nが表す世代nよりも古い世代である場合、 ステップS1005に進む。

一方、ステップS1002において、暗号文保持部102に記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代n以後であると判定された場合、即ち、暗号文保持部102に記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代nと同一か、又はそれよりも新しい場合、ステップS1003に進み、CPU670は、記録媒体I/F690を制御することにより、暗号文保持部102に記憶された暗号化マスターキーCの世代を表す世代情報を、記録時世代情報とし、記録媒体200(図8参照)に記録させる。

そして、記録媒体200に記録すべきコンテンツが、記録再生装置に入力されると、ステップS1004において、そのコンテンツは、暗号処理手段650で暗号化され、バス610を介して、記録媒体I/F690に供給される。

すなわち、記録媒体 200 に記録すべきコンテンツとしてのディジタル信号が、ディジタル I / F 6 20 に供給されると、ディジタル I / F 6 20 は、そのディジタル信号を、バス 6 10 を介して、暗号処理手段 6 50 (図 7 参照)のエンコーダ 701 に供給する。また、記録媒体 200 に記録すべきコンテンツとしてのアナログ信号が、アナログ I / F 6 40 に供給されると、そのアナログ信号は、コンバータ 6 35 を介することにより、ディジタル信号とされ、MPEGコーデック 6 30 に供給される。そして、MPEGコーデック 6 30 において、コンバータ 6 35 からのディジタル信号がMPEGエンコードされ、バス 6 10 を介して、暗号処理手段 6 50 のエンコーダ 701 に供給される。

暗号処理手段650では、マスターキー復号部103において、暗号文保持部102に記憶されている暗号化マスターキーCが、デバイスキー保持部101に記憶されているデバイスキーDKに基づいて、マスターキーMKに復号され、エンコーダ701に供給される。エンコーダ701では、マスターキー復号部103からのマスターキーMKを用いて、そこに供給される平文のディジタル信号(コンテンツ)が暗号化され、その結果得られる暗号化コンテンツが、バス61

0を介して、記録媒体I/F690に供給される。

さらに、ステップS1004では、記録媒体 I/F690において、暗号処理手段650からの暗号化コンテンツが、記録媒体200に供給されて記録され、処理を終了する。

なお、例えば、記録媒体200が、光ディスク等のディスク形状の記録媒体である場合には、記録時世代情報は、例えば、図11に示すように、セクタのセクタヘッダ等に記録される。すなわち、セクタは、セクタヘッダとユーザデータ部とから構成され、記録時世代情報は、その記録時世代情報が表す世代のマスターキーMKで暗号化された暗号化コンテンツが、ユーザデータ部に記録されるセクタのセクタヘッダに記録される。ここで、このような世代情報の記録方法については、本件出願人が先に提案している特願平10-352975号に、その詳細を記載している。

また、記録媒体200に対して、暗号化コンテンツを、ファイルとして記録する場合には、記録時世代情報は、そのファイルと対応付けて管理することができるような形で、記録媒体200に記録することができる。

ここで、上述の場合には、暗号文保持部102に記憶された世代のマスターキーを用いて、コンテンツを暗号化して記録するようにしたが、その他、例えば、暗号文保持部102に記録された世代のマスターキーから、記録媒体200に記録されているプレ記録世代情報が表す世代のマスターキーを生成し、そのマスターキーを用いて、コンテンツを暗号化して記録することも可能である。この場合、記録媒体200に記録されるコンテンツの暗号化に用いられるマスターキーの世代は、その記録媒体200に記録されているプレ記録世代情報が表す世代に、必ず一致するから、記録時世代情報は、記録媒体200に記録する必要がなくなる。一方、ステップS1005に進んだ場合、暗号文保持部102に記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代 n よりも古い世代である場合には、記録媒体200へのデータの記録は許可されない(行うことができない)。

このため、ステップS1005では、ユーザI/F660を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示、又は音

声出力等により、警告音、警告表示の出力を実行して処理を終了する。

これにより、ユーザがこのメッセージに従って、例えば、機器メーカーのサービスステーションに機器を持ち込んでマスターキーを更新したり、下記の実施例に述べる方法でマスターキーを更新することによって、次回以降、この記録媒体200へのデータの記録が行えるようになる。

(2.6. コンテンツ再生処理)

次に、図12のフローチャートを参照して、記録媒体200からのデータの再 生が行われる場合の、記録再生装置の動作について説明する。

まず最初に、ステップS1201において、記録媒体 I/F690は、記録媒体 200 から、プレ記録世代情報Generation#nを読み出し、CPU670に供給する。さらに、記録媒体 I/F690は、ステップS1202に進み、再生しようとしているコンテンツ(データ)の暗号化に用いられたマスターキーMKの世代情報(記録時世代情報)を、記録媒体 200 から読み出し、CPU670に供給する。

CPU670は、ステップS1203において、記録媒体I/F690からのプレ記録世代情報Generation#nが表す世代nと、記録時世代情報が表す世代mとを比較し、その世代の前後を判定する。

ステップS1203において、記録時世代情報が表す世代mが、プレ記録世代情報Generation#nが表す世代n以後でないと判定された場合、即ち、記録時世代情報が表す世代mが、プレ記録世代情報Generation#nが表す世代nよりも古い世代である場合、ステップS1204乃至S1206をスキップして、処理を終了する。

したがって、記録媒体200に記録されたコンテンツが、プレ記録世代情報Ge naration#nが表す世代nよりも古い世代のマスターキーMKに基づいて暗号化されたものである場合には、その再生は行われない(再生は許可されない)。

すなわち、この場合は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体200に記録された場合に該当するから、そのような不正な装置によってデータが記録された記録媒体200の再生は行われないようにな

っており、これにより、不正な記録装置の使用を排除することができるようになっている。

一方、ステップS1203において、記録時世代情報が表す世代mが、プレ記録世代情報Generation#nが表す世代n以後であると判定された場合、即ち、記録時世代情報が表す世代mが、プレ記録世代情報Generation#nが表す世代nと同一か、又は新しい世代であり、従って、記録媒体200に記録されたコンテンツが、プレ記録世代情報Generation#nが表す世代n以後の世代のマスターキーMKに基づいて暗号化されたものである場合には、ステップS1204に進み、CPU670は、暗号処理部650(図7)の暗号文保持部102が記憶している暗号化マスターキーCの世代を認識し、その暗号化マスターキーの世代と、記録時世代情報が表す世代mを比較して、その世代の前後を判定する。

ステップS1204において、暗号文保持部102に記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代m以後でないと判定された場合、即ち、暗号文保持部102に記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代mよりも古い世代である場合、ステップS1207に進む。

一方、ステップS1204において、暗号文保持部102に記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代m以後であると判定された場合、即ち、暗号文保持部102に記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代mと同一か、又はそれよりも新しい場合、ステップS1205に進み、暗号処理手段650(図7参照)のマスターキー復号部103において、暗号文保持部102に記憶されている暗号化マスターキーCが、デバイスキー保持部101に記憶されているデバイスキーDKに基づいて、マスターキーMKに復号される。さらに、マスターキー復号部103は、その復号したマスターキーMKの世代が、記録時世代情報が表す世代mよりも新しい場合には、上述したようにして、復号したマスターキーMKから、記録時世代情報が表す世代mのマスターキーMKを生成し、デコーダ702に供給する。

そして、ステップS1206に進み、記録媒体I/F690は、記録媒体200から暗号化コンテンツを読み出し、バス610を介して、暗号処理手段650に供給する。さらに、ステップS1206では、暗号処理手段650のデコーダ

702において、記録媒体200からの暗号化コンテンツが、ステップS120 5で得られたマスターキーMKに基づいて復号され、処理を終了する。

一方、ステップS1207では、暗号文保持部102に記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代mよりも古い世代であるので、記録媒体200からのデータ再生は許可されない。すなわち、暗号化マスターキーCの世代が、記録時世代情報が表す世代mよりも古い世代である場合には、上述したように、暗号化マスターキーCから得られるマスターキーMKから、その世代よりも新しい世代mのマスターキーMKを生成することはできないため、記録媒体200からのデータの再生は行われない(行うことができない)。

このため、ステップS1207では、ユーザI/F660を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示して処理を終了する。すなわち、ユーザI/F660を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示、又は音声出力等により、警告音、警告表示の出力を実行して処理を終了する。

これにより、ユーザがこのメッセージに従って、例えば、機器メーカーのサービスステーションに機器を持ち込んでマスターキーを更新したり、下記の実施例に述べる方法でマスターキーを更新することによって、次回以降、この記録媒体200からのデータの再生が行えるようになる。

以上のように、記録時世代情報が表す世代が、プレ記録世代情報が表す世代以後の世代でない場合には、再生を行うことができないようにしたので、マスターキーの更新を、いわば強制することができ、これにより、不正な装置により記録が行われた記録媒体の流通を、間接的に排除することができる。

また、機器が最新のマスターキーを記憶していないためにある記録媒体へのデータの記録又は再生が行えない場合には、ユーザにマスターキーの更新を促すメ

ッセージを表示し、システム全体でのマスターキーの更新作業をさらに加速する ことができる。

- [3. その他の実施例]
- (3.1. I Cカードによるマスターキー更新構成)

次に、本発明を適用した記録再生装置の別の実施例の形態の構成例を図13に示す。

図13の各構成要素の大部分は図6と同様であり、説明を省略する。図13において、バス610には I C (Integrated Curcuit) カード I / F 1301が接続されている。 I Cカード I / F 1301は、記録再生装置に着脱可能な I Cカード 1302とデータをやりとりするためのインタフェースである。

記録媒体200が、この記録再生装置にセットされたとき等に行われるマスターキーの更新処理は、図9と同様である。

次に、図14のフローチャートを参照して、記録媒体200に対するデータの 記録が行われる場合の、記録再生装置の動作について説明する。

図14において、ステップS1401乃至S1405の処理は、図10のステップS1001乃至S1005の各処理と同様であるため、説明を省略する。但し、ステップS1405においては、ユーザに対してマスターキーの更新を促すメッセージを表示した後、ステップS1406に進む。すなわち、ユーザI/F660を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示、又は音声出力等により、警告音、警告表示の出力を実行してステップS1406に進む。

ステップS1406では、ICカード1302がユーザによって装置に装着されるのを待ち、そしてICカード1302を用いてマスターキーの更新を行う。すなわち、ICカード1302には、図8を用いて説明した記録媒体200に記録されているのと同様のキーテーブルが格納されており、これを上述の方法を用いて処理することにより、最新世代の暗号化マスターキーを記録再生装置が得ることが可能である。

上記例では、I Cカード1302には、図8を用いて説明した記録媒体200 に記録されているのと同様のキーテーブルが格納されているとしたが、これは以 下のようなものであってもよい。

すなわち、記録再生機器のメモリ680には個々の記録再生機器を識別するための識別情報 (機器 I D) と、個々の機器 I Dに対応するデバイスキーが格納されており、I Cカード1302には、機器 I Dと、最新世代のマスターキーを個々の機器 I Dに対応するデバイスキーで暗号化した暗号化マスターキーが格納されている。これを記録媒体 2 0 0 に格納されているキーテーブルと同様に取り扱うことによって、最新世代の暗号化マスターキーを記録再生装置が入手することが可能である。

I Cカードはキー発行機関が、個々のユーザ毎に個々のデータを格納して郵送するなどの方法がとりやすいため、このように I Cカードを用いることにより、よりきめこまかな鍵の管理が行え、記録媒体の記録容量をキーテーブルで消費してしまうことがないという利点を持つ。

次に、ステップS1407では、ステップS1406で必要な世代の暗号化マスターキーがICカード51を介して取得できたかどうかの検査を行う。

もし必要な世代の暗号化マスターキーが取得できていれば、ステップS140 3に進み、最終的に記録媒体200へのデータの記録を行う。

必要な世代の暗号化マスターキーが取得できなければ、データの記録は行わず に処理を終了する。なお、この際に、必要な世代の暗号化マスターキーが取得で きなかった旨のメッセージをユーザに対して表示してもよい。

次に、図15のフローチャートを参照して、記録媒体200に記録されたデータの再生が行われる場合の、記録再生装置の動作について説明する。

図15において、ステップS1501乃至S1507の処理は、図12のステップS1201乃至S1207の各処理と同様であるため、説明を省略する。但し、ステップS1507においては、ユーザに対してマスターキーの更新を促すメッセージを表示した後、ステップS1508に進む。すなわち、ユーザI/F660を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示、又は音声出力等により、警告音、警告表示の出力を実行してステップS1508に進む。

ステップS1508では、図14のステップS1406と同様にして、必要な

世代の暗号化マスターキーをICカード51から取得する。そして、ステップS1509に進む。

ステップS1509では、ステップS1508で必要な世代の暗号化マスターキーを取得できたか否かの検査を行う。

もし必要な世代の暗号化マスターキーが取得できていれば、ステップS150-5に進み、最終的に記録媒体200からのデータの再生を行う。

必要な世代の暗号化マスターキーが取得できなければ、データの記録は行わず に処理を終了する。なお、この際に、必要な世代の暗号化マスターキーが取得で きなかった旨のメッセージをユーザに対して表示してもよい。

(3.2.モデムを介するマスターキー更新構成)

次に、本発明を適用した記録再生装置の別の実施例の形態の構成例を図16に 示す。

図16の記録再生装置1600の各構成要素の大部分は図6と同様であり、説明を省略するが、メモリ680には、記録再生装置固有の識別情報(機器ID)と、機器ID毎に固有の、共通鍵暗号系の暗号鍵又は、公開鍵暗号系の秘密鍵と公開鍵証明書などが格納されている。

図16において、バス610にはモデム1601が接続されており、モデム1 601は電話回線と接続されている。

次に、図17のフローチャートを参照して、図16の構成を有する記録再生装置1600における記録媒体200に対するデータの記録が行われる場合の、記録再生装置1600の動作について説明する。

図17において、ステップS1701乃至S1704の処理は、図10のステップS1001乃至S1004の各処理と同様であるため、説明を省略する。

ステップS1702において、自身が格納する暗号化マスターキーの世代が、プレ記録世代情報よりも古いと判定された場合、ステップS1705において、記録再生装置はモデム1601を使用してキー発行機関と電話回線を介してリンクを張り、キー発行機関が送信した最新世代の暗号化マスタキーを受信して取得する。

なお、この際に、記録再生装置とキー発行機関が互いに相手の正当性を確認す



るために、相互認証のプロトコルを実行してもよい。相互認証のプロトコルの例としては、ISO/IEC 9798-2 に代表される、共通鍵暗号を用いるもの、ISO/IEC 9798-3に代表される、公開鍵暗号を用いるもの、ISO/IEC 9798-4 に代表される、暗号学的チェック関数を用いるものなどが挙げられる。

図18は、暗号学的チェック関数を用いた相互認証及び暗号鍵共有のための方法のひとつを本実施例に用いたものである。

図18において、記録再生機器 (Device B と表す) は、固有の機器 I D: I D _Bと、秘密鍵 D K _Bを格納している。またキー発行機関 A は、それぞれの機器 O と、それぞれの機器 I D に対応する秘密鍵のテーブルを保存している。

まず、記録再生装置は乱数 R_B を発生し、 ID_B とともにキー発行機関に送る。なお、図18における記号「||」は連結を表している。

次にキー発行機関は、乱数 R_A 、 S_A を生成し、 R_A , S_A , ID_A とともにMA $C(DK_B$, $R_A \mid\mid R_B \mid\mid S_A)$ を記録再生装置に送る。 ID_A はキー発行機関を表す識別情報であり、 $MAC(DK_B$, $R_A \mid\mid R_B \mid\mid S_A)$ は、暗号学的チェック関数に鍵として DK_B を、データとして $R_A \mid\mid R_B \mid\mid S_A$ を入力することを表す。暗号学的チェック関数は、ISO/IEC 9797 に示されているように、FIPS 46-2 のデータ暗号化規格(Data Encryption Standard, DES)を用いて構成することが可能である。またこの際使用する DK_B は格納されているテーブルから ID_B を検索キーとして検索してくる。

記録再生装置は、受信したデータを用いて自分でもMAC(DK_B, R_A || R_B || S_A)を計算し、これが受信したものと一致するかを検査する。一致すれば、キー発行機関が正当なものとして認め、処理を続けるが、一致しなければキー発行機関が不正なものと判断して処理を中止する。

次に記録再生装置は乱数 S_Bを生成し、これとMAC(DK_B, R_B | R_A | S_B)をキー発行機関に送る。

キー発行機関も受信したデータを用いて自分でMAC(DK_B, R_B || R_A || S_B)を計算し、受信したものと一致するかを確認する。一致すれば、記録再生装置が正当なものとして認め、処理を続けるが、一致しなければ記録再生装置が不正なものと判断して処理を中止する。

最後に、双方が $MAC(DK_B, S_A \mid\mid S_B)$ を計算し、これをそのセッションにおけるセッションキーとして使用する。

上記のようにすることにより、キー発行機関と記録再生装置は互いの正当性を 検査することができ、またセッションキーを安全に共有することができたので、 例えば、このセッションキーを鍵として、最新世代のマスターキーをDESなど で暗号化してキー発行機関が記録再生機器に安全に送信することが可能となる。

図19は、公開鍵暗号を用いた認証技術を本実施例に適用したものである。

図19において、キー発行機関A及び記録再生装置Bは、それぞれ自分の識別情報であるIDと、自分の公開鍵証明書、及びリポケーションリスト又はレジストレーションリストを持っている。公開鍵証明書は、図20に示すように、そのエンティティのIDと、公開鍵に対し、センタ (キー発行機関) が署名を施したデータである。

リポケーションリストは、不正者リストあるいはブラックリストとも呼ばれ、 図21に示すように、その装置の秘密鍵が露呈してしまったもののIDがリスト アップされ、単調増加するバージョンナンバとともにセンタ (キー発行機関) の ディジタル署名が施されたものである。

これに対し、レジストレーションリストは、正当者リストあるいは登録リストとも呼ばれ、図22に示すように、その時点で信頼できる(秘密が露呈していない)装置のIDがリストアップされ、単調増加するバージョンナンバとともにセンタ(キー発行機関)のディジタル署名が施されたものである。

図19において、記録再生装置は乱数 R_B を発生させ、キー発行機関に送る。キー発行機関は、乱数 K_A 及び R_A を発生させ、楕円曲線E上でシステム共通の点(ベースポイント)であるGと K_A を乗算して V_A を計算し、さらに自分の秘密鍵($PriKey_A$)を用いてデータ R_A || R_B || V_A に対して施した署名とともに、公開鍵証明書($Cert_A$, R_A , R_B , V_A) を記録再生装置に送る。

記録再生装置は、キー発行機関の公開鍵証明書の正当性、キー発行機関が作成した署名の正当性を検査する。そして、自分がリボケーションリストを格納していれば、相手のIDがリボケーションリストに載っていないことを、また、自分がレジストレーションリストを格納していれば、相手のIDがレジストレーショ

ンリストに登録されていることを確認する。以上の確認が正常にできなければ、記録再生装置はキー発行機関が不正者と判断して処理を終了する。以上の確認が正常にできれば、記録再生装置は、乱数 K_B を生成して、キー発行機関が行ったのと同様な計算を行い、公開鍵証明書($Cert_B$, R_B , R_A , V_B)とともにデータ $R_B \parallel R_A \parallel V_B$ に対して施した署名をキー発行機関に送る。

キー発行機関では、上で記録再生装置が行ったのと同様の検査を受信したデータに対して行い、全ての検査が正常に終了したときのみ処理を継続する。

この後、キー発行機関では K_A と V_B を、記録再生装置では K_B と V_A を、それぞれ楕円曲線E上で乗算してセッションキー K_S を得る。セッションキーの使用方法については、上述の図18と同様である。

なお、楕円曲線上の乗算やディジタル署名の生成及び検査方法については、現在 IEEE P1363 で規格制定中であり、そのドラフトに詳細が記されている。

図17に戻り、ステップS1706に進み、必要な世代のマスターキーを記録 再生装置が入手できたか否かを検査する。入手できていれば、ステップS170 3に進み、結局記録媒体へのデータの記録を行う。

必要な世代の暗号化マスターキーが取得できなければ、データの記録は行わず に処理を終了する。なお、この際に、必要な世代の暗号化マスターキーが取得で きなかった旨のメッセージをユーザに対して表示してもよい。

なお、上記の例では、ステップS1705において、モデム1601を用い、 電話回線を使用してキー発行機関からマスターキーを得るようにしているが、他 の記録再生装置から得ることも可能であり、また、モデム52ではなくディジタ ルI/F620を介したリンクからでもよい。キー発行機関からではなく、他の 記録再生装置とマスターキーの授受を行う場合には、図19に示した、公開鍵を 用いた認証方式を用いることが好適である。

次に、図23のフローチャートを参照して、記録媒体200に記録されたデータの再生が行われる場合の、図16に示す記録再生装置1600の動作について説明する。

図23において、ステップS2301乃至S2306の処理は、図12のステップS1201乃至S1206の各処理と同様であるため、説明を省略する。但

し、ステップS2304においては、再生装置が格納する暗号化マスターキーの世代が、記録時世代情報に表される世代よりも古い場合には、ステップS2307に進む。

ステップS2307では、図17のステップS1705と同様の方法を用いて、 最新世代の暗号化マスターキーの取得を試みる。すなわち、記録再生装置1600はモデム1601を使用してキー発行機関と電話回線を介してリンクを張り、 キー発行機関が送信した最新世代の暗号化マスターキーを受信して取得する。なお、この際に、記録再生装置とキー発行機関は、上述の相互認証のプロトコルを 実行することが好ましい。

次に、ステップS2308では、ステップS2307において必要な世代の暗号化マスターキーを取得できていればステップS2305に進み、結局記録媒体200からデータの読み出しを行う。一方、必要な世代の暗号化マスターキーを取得できていなければ、データの読出しを行わずに処理を終了する。なお、この際に、必要な世代の暗号化マスターキーが取得できなかった旨のメッセージをユーザに対して表示してもよい。

なお、前述の図13万至図15を用いて説明したICカードを使用したマスターキー更新処理においても、記録再生装置1300とICカード1302間の機器間相互認証処理を実行して、認証が成立したことを条件として更新マスターキーの取得処理を実行する構成としてもよい。また、先に説明した図6の構成を持つ記録再生装置600においても、例えばディジタルI/F620を介したネットワーク通信により、マスターキーを取得する際に、上述の認証処理を実行して、その認証が成立した場合にのみ、更新マスターキーの取得処理を実行する構成とすることが好ましい。

(3.3.キー更新端末を介するマスターキー更新構成)

次に、本発明の実施例として、情報記録又は再生装置と別体な独立した機器として構成されるキー更新端末を用いた構成例を説明する。具体的には、前述の図 10のS1005において、最新マスターキーの取得を促すメッセージが表示された場合に、マスターキーの更新をするため、特殊なツール、即ち、キー更新端末を使用してマスターキー更新を行う構成である。キー更新端末は、例えばサー

ビスセンタから派遣されるサービスマンが保有する。本実施例は、このようなキー更新端末を用いた構成である。

前述したように、記録媒体を用いたキー更新構成においては、ひとつのカテゴリに複数、例えば数千台の装置が属する構成である。したがって、1つのカテゴリに含まれる多数の記録再生装置中の1台でも内部に安全に格納すべきデバイスキーが暴かれた場合、このカテゴリに含まれる全ての装置をシステムから排除しなくてはならない。本実施例のキー更新構成では、一旦、排除された装置のうち排除されるべきでない装置をシステム内に復活、即ちキー更新端末を利用してマスターキーの更新を行うことにより再び正常な記録再生を可能とした構成である。以下、キー更新端末を利用したマスターキー更新構成の複数の態様について説明する。

(3.3.1.キー更新端末を介するマスターキー更新構成例-1)

まず、前述の図6と同様の構成を持つ情報記録又は再生装置において、キー更新端末を介するマスターキーの更新処理を行う構成について説明する。但し、本実施例構成においては、情報記録又は再生装置は、装置の属するカテゴリ番号と、それに対応する鍵としてのデバイスキーに加えて、装置固有の識別番号としてのデバイスID(Device ID)と、デバイスIDに対応する装置固有鍵としてのデバイス固有キー(Device Unique Key)を安全に格納している。デバイス固有キーは、例えば先に説明した図1の暗号処理部内に格納される。

本実施例の構成では、情報記録又は再生装置のマスターキーを更新するため、 キー更新用の情報処理装置(以下これをキー更新端末と呼ぶ)を用いる。キー更 新端末の構成例を示すブロック図を図24に示す。

図24に示すように、キー更新端末2400は、制御部2401、モデム2402、ディジタルインタフェース (I/F) 2403を有する。図24のキー更新端末2400は、例えば、前述した通常の記録媒体を用いたキー更新において、その装置の属するカテゴリがリポークされ、カテゴリの識別により更新対象から排除され、その装置が新しいマスターキーを得られない場合に、個々の記録再生、装置が、直接キー発行機関からマスターキーを得るための通信路を提供する。

図25に、情報記録又は再生装置が図24のキー更新端末を用いてキー発行機関からマスターキーを得るための通信路を確立する処理構成を示す。記録再生機装置2500はディジタルI/F2501を有する。このディジタルI/F2501は、通常、音楽や映画などのコンテンツデータを伝送するのに用いられるが、キー発行機関からマスターキーを得る場合とは、このディジタルI/F2501と、キー更新端末2400のディジタルI/F2403を結び、キー更新端末2400のモデム2402により電話回線を介してキー発行機関までの通信路を確立する。制御部2401は、通信制御、通信データのフォーマット変換処理制御、通信データの選択処理制御等を実行する。

キー更新端末2400を介して、記録再生機装置2500がキー発行機関との通信路を確立した後は、図26に示す、共通鍵暗号技術を用いた相互認証及び鍵共有プロトコル、又は、図27に示す、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを用いてキー発行機関と記録再生装置は互いの正当性を確認した後、キー発行機関が記録再生装置に最新のマスターキーを与える。

図26、図27は、先に説明した図18の共通鍵暗号技術を用いた相互認証及び鍵共有プロトコル、図19の公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルと同様の処理シーケンスであるので、詳細な説明は図18,19を参照されたい。但し、図26に示す共通鍵暗号技術を用いた相互認証及び鍵共有プロトコルにおいては、図18の処理シーケンスにおいて秘密鍵として用いたデバイスキー(DK)に変えて、記録再生装置の各々に固有なキーであるデバイス固有キー(DUK)を秘密鍵とした処理を実行する。したがって、キー発行機関は、個々の記録再生装置の機器IDと対応するデバイス固有キーとのテーブルを持つ。

図26又は図27の相互認証、鍵共有プロトコルは、図25で示すキー更新端末2400を介して記録再生機装置2500とキー発行機関との間で実行される。これらの処理の後の更新マスターキーの送信には、上記プロトコルにおいて共有したセッションキーK_Sで更新マスターキーを暗号化して送信することで安全な更新マスターキーの伝送が可能である。

なお、キー発行機関から記録再生装置に対して、認証を行った後に更新マスタ ーキーを伝送するのではなく、相互認証を省略して、記録再生装置の機器 I D

(Device ID) のみを更新要求を行う記録再生装置から受信して、キー 発行機関が有する、機器IDとデバイス固有キーとのテーブルから、個々の記録 再生装置のデバイス固有キー (DUK:Device Unique Key) を取り出して、デバイス固有キー (DUK)でマスターキーを暗号化して各記録 再生装置に送信する構成としてもよい。暗号化されたマスターキーを受信した記し 録再生装置は、自身の有するデバイス固有キー(DUK)で復号して更新マスタ ーキーを取得する。この場合、記録再生装置が通信をする相手は、キー発行機関 のように信頼が必要なものではなく、単に図28のようなマスターキーテーブル を格納しているサーバなどでもよい。図28のテーブルは、1つのカテゴリ内の 個々の記録再生装置に対応付けて生成されたテーブルであり、記録再生装置の機 器IDである装置固有識別番号と、対応する記録再生装置のデバイス固有キー (DUK) で暗号化された第n世代のマスターキー (MK_n) が対応付けられ て格納されたテーブルである。マスターキーの更新を実行する記録再生装置は、 キー更新端末を介して図28に示すテーブルを格納したサーバにアクセスして、 自身のデバイス固有キー (DUK) で暗号化された第n世代のマスターキー (M K_n) を取得する。

(3.3.2.キー更新端末を介するマスターキー更新構成例-2)

次に、キー更新端末を介するマスターキー更新構成例の第2の実施例として、 記録再生装置の通信インタフェース (I/F) にキー更新端末に接続して更新マ スターキーを取得する構成例を説明する。

本実施例における記録再生装置は、図29に示すように記録再生装置2900の通信I/F2901を介してキー更新端末2950の通信I/F2951に接続し、前述の例と同様に制御部2951の制御のもとにモデム2952を介して鍵発行機関と接続して、前述の相互認証処理、鍵共有プロトコルを実行して、更新マスターキーを取得する。記録再生装置2900の通信I/F2901は、赤外線通信やブルートゥース(Bluetooth)などの無線通信方式とすることも可能である。

(3.3.3.キー更新端末を介するマスターキー更新構成例 - 3) 上述した2つの例では、鍵発行センタとの通信路をキー更新端末を介して確立 して通信により、更新マスターキーを取得していた。第3の例は、キー更新端末が、記録再生装置とキー発行機関の間の通信路を確立するのではなく、それ自体がキー発行機関もしくは上記のサーバとして働く。すなわち、キー更新端末中に、記憶手段を持っており、例えば図28に示したマスターキーテーブルを記憶手段に格納した構成を持つ。

図30及び図31に本構成例の更新マスターキーの取得処理を説明する図を示す。図30において、記録再生機装置3000はディジタルI/F3001を有する。このディジタルI/F3001は、通常、音楽や映画などのコンテンツデータを伝送するのに用いられるが、キー更新端末3050からマスターキーを得る場合には、このディジタルI/F3001と、キー更新端末3050のディジタルI/F3053を結び、キー更新端末3050の記録媒体3053に格納された、例えば図28に示す暗号化マスターキー格納テーブルから、自身の機器IDに対応する暗号化マスターキーを取得する。制御部3051は、記録再生機装置3000とキー更新端末3050間の通信制御等を実行する。

また図31に示すように記録再生装置3100の通信I/F3101を介してキー更新端末3150の通信I/F3151に接続し、前述の例と同様にキー更新端末3150の記録媒体3153に格納された、例えば図28に示す暗号化マスターキー格納テーブルから、自身の機器IDに対応する暗号化マスターキーを制御部3151の制御のもとに取得する。記録再生装置3100の通信I/F3101は、赤外線通信やブルートゥース(Bluetooth)などの無線通信方式とすることも可能である。

また本例においても、キー更新端末と記録再生装置が相互認証及び鍵交換プロトコルを実行し、互いの正当性を確認した後に、上記プロトコルで共有した暗号鍵を用いてキー更新端末が記録再生装置に安全にマスターキーを伝送する構成としてもよい。この際の処理は、先に説明した図26の共通鍵暗号技術に基づいた認証及び鍵交換プロトコル又は図27の公開鍵暗号技術に基づいた認証及び鍵交換プロトコルを適用することが可能である。

図26の共通鍵暗号技術に基づいた認証及び鍵交換プロトコルを用いる場合には、キー更新端末にデバイス固有キー(DUK: Device Unique

Key)テーブルを持たせておき、さらにデバイス固有キー (DUK) が露呈したことがわかっている記録再生装置の機器ID (Device ID) にはその旨のマークをつけておき、マスターキーを渡さないようにする。

また図27の公開鍵暗号技術に基づいた認証及び鍵交換プロトコルを用いる場合には、キー更新端末にデバイス固有キー(DUK: Device Unique Key)テーブルは必要ないが、やはりデバイス固有キー(DUK)が露呈したことがわかっている記録再生装置にマスターキーを渡さないために、それらの機器ID(Device ID)をリストにしたリボケーションリストをキー更新端末に格納しておき、キー更新要求のあった記録再生装置の機器IDに対応する危機IDがリストに載っていない装置にのみマスターキーを渡すようにする。

このように、キー更新端末を介するマスターキー更新構成を用いることにより、記録再生器とは別体として構成されるキー更新端末装置を介する更新キーの入手が可能となり、例えば、同一カテゴリに属する他の機器のデバイスキーの露呈によってマスターキーの更新が必要となった機器が、キー更新端末を介してキー発行機関と通信路を確立して、もしくは、キー更新端末から直接、マスターキーを入手することが可能となり、同一のカテゴリに属する端末中の個々の端末に対して個別の対応が可能となる。また、キー更新端末は、記録再生機器とは別に、更新処理を必要とする場合にのみ記録再生器に接続して使用する構成とすればよく、記録再生装置に通常備わるインタフェースを介して情報をやりとりできるため、記録再生装置にモデムなどを設けてコストアップさせる必要がない点でも優れている。

[4.キー配信構成としてのツリー (木) 構造について]

次に、図6に示した記録再生装置が、データを記録媒体に記録、もしくは記録 媒体から再生する際に必要なマスターキーを、ツリー構造の鍵配信構成を用いて 各機器に配布する構成について説明する。図32は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図32の最下段に示すナンバ0~15が個々の記録再生装置である。すなわち図32に示す木(ツリー)構造の各葉(リーフ:leaf)がそれぞれの記録再生装置に相当する。 各デバイス $0\sim15$ は、製造時(出荷時)に、予め定められている初期ッリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)及び各リーフのリーフキーを自身で格納する。図32の最下段に示す $K0000\sim K1111$ が各デバイス $0\sim15$ にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節(ノード)に記載されたキー: $KR\sim K111$ をノードキーとする。

図32に示すツリー構成において、例えばデバイス0はリーフキーK0000 と、ノードキー: K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図32のツリーにはデバイスが0~15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図32のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック(商標)等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図32に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシスチムにおいて、例えば図32の点線で囲んだ部分、即ちデバイス0,1,2,3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行う機関は、図32の点線で囲んだ部分、即ちデバイス0,1,2,3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図32のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行うプロバイダ、 決済機関等によってグループ毎に管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図32から明らかなように、1つのグループに含まれる3つのデバイス0,1,2,3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0,1,2,3のみに提供することが可能となる。例えば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0,1,2,3のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーK00で暗号化した値Enc(K00,Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0,1,2,3に配布すれば、デバイス0,1,2,3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00,Kmaster)を解いてマスターキー:Kmasterを得ることが可能となる。なお、Enc(Ka,Kb)はKbをKaによって暗号化したデータであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図33(A)に示すキー更新ブロック (KRB: Key Renewal Block) と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納

してデバイス0, 1, 2に供給することによって実行される。

図33(A)に示すキー更新ブロック(KRB)には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図33の例は、図32に示すツリー構造中のデバイス0,1,2において、世代 t の更新ノードキーを配布することを目的として形成されたブロックデータである。図32から明らかなように、デバイス0,デバイス1は、更新ノードキーとしてK(t)00、K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)00、K(t)0、K(t)R が必要である。

図33(A)のKRBに示されるようにKRBには複数の暗号化キーが含まれ る。最下段の暗号化キーは、Enc (K0010, K (t) 001) である。こ れはデバイス2の持つリーフキーΚ0010によって暗号化された更新ノードキ -K (t) 001であり、デバイス2は、自身の持つリーフキーによってこの暗 号化キーを復号し、K(t)001を得ることができる。また、復号により得た K (t) 001を用いて、図33 (A) の下から2段目の暗号化キーEnc (K (t) 001, K(t) 00) を復号可能となり、更新ノードキーK(t) 00 を得ることができる。以下順次、図33(A)の上から2段目の暗号化キーEn c (K (t) 00, K (t) 0) を復号し、更新ノードキーK (t) 0、図33 (A) の上から1段目の暗号化キーEnc(K(t)0,K(t)R)を復号し K(t) Rを得る。一方、デバイス0,1は、ノードキーK000は更新する対 象に含まれておらず、更新ノードキーとして必要なのは、K (t)00、K (t) 0、K(t) Rである。テバイス0,1は、図33(A)の上から3段目 の暗号化キーEnc(K000, K(t)00)を復号しK(t)00を取得し、 以下、図33(A)の上から2段目の暗号化キーEnc(K(t)00,K (t) 0) を復号し、更新ノードキーK(t) 0、図33(A) の上から1段目 の暗号化キーEnc(K(t)0,K(t)R)を復号しK(t)Rを得る。こ のようにして、デバイス0, 1, 2は更新した鍵K (t) 00, K (t) 0, K(t) Rを得ることができる。なお、図33 (A) のインデックスは、復号キー として使用するノードキー、リーフキーの絶対番地を示す。

図33(B)に示すKRBは、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図32に点線で示すグループ内のデバイス0,1,2,3がある記録媒体を用いており、新たな共通のマスターキーK(t)masterが必要であるとする。このとき、デバイス0,1,2,3の共通のノードキーK00を更新したK(t)00を用いて新たな共通の更新マスターキー:K(t)masterを暗号化したデータEnc(K(t),K(t)master)を図33(B)に示すKRBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス 0 、 1 、 2 は K R B を処理して得た K (t) 0 0 を用いて上記暗号文を復号すれば、 t 時点でのマスターキーK (t) master を得ることが可能になる。

[KRBを使用したマスターキーの配布]

図34に、 t時点でのマスターキーK (t) masterを得る処理例として、K (t) 00を用いて新たな共通のマスターキーK (t) masterを暗号化したデータEnc(K(t)00,K(t)master)と図33(B)に示すKRBとを記録媒体を介して受領したデバイス0の処理を示す。

図34に示すように、デバイス0は、記録媒体に格納されている世代: t時点の KRBと自分が予め格納しているノードキーK000を用いて上述したと同様の KRB処理により、ノードキーK(t)00を生成する。さらに、復号した更新 ノードキーK(t)00を用いて更新マスターキーK(t) masterを復号して、後にそれを使用するために自分だけが持つリーフキーK0000で暗号化して格納する。なお、デバイス0が更新マスターキーK(t) master を安全に自身内に格納できる場合、リーフキーK0000で暗号化する必要はない。

また、この更新マスターキーの取得処理を図35のフローチャートにより説明

する。なお、記録再生装置は出荷時にその時点で最新のマスターキー: K (c) masterを与えられ、自身のメモリに安全に(具体的には例えば、自身のリーフキーで暗号化して)格納しているものとする。

更新マスターキーK(n) masterとKRBの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップS3501において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキーK(n) masterの時点(世代)番号:n(これを、プレ(pre-recording)記録世代情報(Generation#n)と呼ぶことにする)を読み出す。記録媒体には、予め、マスターキーK(n) masterの時点(世代)番号:nが記憶されている。また、自身が保持している暗号化マスターキーCを読み出し、ステップS3502において、その暗号化マスターキーの世代:cと、プレ記録世代情報Generation#nが表す世代:nとを比較して、その世代の前後を判定する。

ステップS3502において、プレ記録世代情報Generation#nが表す世代: nの方が、自身のメモリに記憶された暗号化マスターキーCの世代: cよりも後でない (新しくない)と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代: cが、プレ記録世代情報Generation#nが表す世代: nと同一か、又は後の場合、ステップS3503乃至S3508をスキップして、マスターキー更新処理を終了する。すなわち、この場合、自身のメモリに記憶されたマスターキーK(c)master(暗号化マスターキーC)の更新は行う必要がないので、その更新は行われない。

一方、ステップS 3 5 0 2 において、プレ記録世代情報Generation和が表す世代: nの方が、メモリに記憶された暗号化マスターキーCの世代: cよりも後である (新しい) と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation和が表す世代 nよりも前の世代である場合、ステップS 3 5 0 3 に進み、記録再生装置は、記録媒体から、キー更新プロック (KRB: Key Renewal Block) を読み出す。

ステップS3504において、記録再生装置は、ステップS3503で読み出したKRBと、自身がメモリに格納しているリーフキー(図32のデバイス0におけるK0000)及びノードキー(図32のデバイス0におけるK0000, K0

0...)を用いて、プレ記録世代情報Generation#n(図34におけるt)時点での ノード00の鍵K(t)00を計算する。

ステップS3505では、ステップS3504においてK(t)00を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリポーク(排除)されていることを示すので、ステップS3506乃至S3508をスキップしてマスターキー更新処理を終了する。

K (t) 00を得られた場合、ステップS3506に進み、記録媒体からEn c (K (t) 00, K (t) master)、即ち、K (t) 00を用いても時点でのマスターキーを暗号化した値を読み出す。そしてステップS3507において、この暗号文をK (t) 00を用いて復号してK (t) masterを計算する。

ステップS3508では、自身のみが持つリーフキー(図32のデバイス0におけるK0000)を用いてK(t) masterを暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

ところで、マスターキーは、時点(世代)0から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数fを保持しており、その一方向性関数fに、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

具体的には、例えば、記録再生装置に記憶されているマスターキーM K O 世代が世代i+1であり、あるデータの再生に必要な(記録時に使用された)マスターキーM K O 世代が世代i-1 である場合、マスターキーK (i-1) masterは、記録再生装置において、一方向性関数 f が 2 回用いられ、 f (f (K (i+1) master))を計算することにより生成される。

また、記録再生装置に記憶されているマスターキーの世代が世代i+1であり、必要なマスターキーの世代が世代i-2である場合、マスターキーK (i-2) masterは、一方向性関数 f を 3 回用いて、 f (f (f (K (i+1) master))) を計算することにより生成される。

ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、MD5(Message Digest 5)や、SHA-1(Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーK(0) master, K(1) master, K(2) master・・・, K(N) masterを、予め求めておく。すなわち、まず最初に、第N世代のマスターキーK(N) masterを設定し、そのマスターキーK(N) masterに、一方向性関数を1回ずつ適用しいくことで、それより前の世代のマスターキーK(N-1) master, K(N-2) master,・・・, K(1) master, K(0) masterを順次生成しておく。そして、世代の小さい(前の)マスターキーK(0) masterを順次生成しておく。そして、世代の小さい(前の)マスターキーを生成するのに用いる一方向性関数は、全ての記録再生装置に設定されているものとする。

また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、全ての再生装置に与えておく。そして、キー発行機関は、第0世代のマスターキーK(0)masterを設定し、そのマスターキーK(0)masterから使用していく。すなわち、キー発行機関は、第1世代以降のマスターキーK(i)masterが必要になったら、その1世代前のマスターキーK(i-1)masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、N世代のマスターキーを、予め生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

[5. 記録再生装置による記録媒体へのキー更新ブロック (KRB) 格納処理]

ところで、上述した例では、キー更新ブロック: KRB (Key Renewal Block)が記録媒体に予め格納されている例を示したが、記録再生装置が入出力 I / F や、I Cカード、モデム等を介して他の機器から受信した KRB (Key Renewal Bloc

k) を、最初に記録媒体にデータを記録する際や、記録媒体にデータを記録するたび毎に記録媒体に記録するようにすることもできる。

すなわち、図36に示すように、記録再生装置は予め、入出力I/Fや、ICカード、モデム等を介してキー更新プロック:KRB(Key Renewal Block)とマスターキーをノードキーで暗号化した暗号文を入手し、自身の記憶手段に格納しておき、コンテンツデータの記録媒体に対する記録の際に、図37に示すフローチャートに従って処理をする構成としてもよい。

図37の処理フローについて説明する。ステップS3701において、データを記録しようとする記録媒体には既にキー更新プロック: KRB (Key Renewal Block)が記録されているか否かを検査する。既に記録媒体にキー更新プロック: KRB (Key Renewal Block)が記録されていた場合にはステップS3702をスキップして終了する(データの記録処理に進む)が、記録されていない場合には、ステップS3702に進み、図38に示すように、自身の記憶手段に格納しているキー更新プロック: KRB (Key Renewal Block)とマスターキーを暗号化した暗号文を記録媒体に記録する処理を実行する。その処理の実行の後に、コンテンッデータの記録処理に進む。

本実施例における記録媒体の構成例を図39に示す。図39に示す記録媒体には、記録媒体世代番号が格納される。この記録媒体3900には、この記録媒体3900に対するデータの記録及び再生に必要なマスターキーMKの最小の世代を表す世代情報としての世代番号(Generation#n)が記録されている。ここで、この世代番号(Generation#n)は、例えば、記録媒体3900の製造時に、予め記録されるものであり、前術のプレ記録世代情報(Pre Recording Generation#n)と同様である。

この図39に示す記録媒体3900に対するデータの記録及び再生に必要なマスターキーMKの最小の世代は世代番号:nである。世代番号:nは例えばシーケンシャルな世代番号として付与される。記録再生装置が自身の記憶手段に格納しているマスターキーの世代がnより以前である場合は、図39に示す記録媒体3900に対する記録、及び記録媒体3900からの再生が拒否される。

世代番号(プレ記録世代番号)が記録された記録媒体3900を記録再生装置

に装着して記録あるいは再生を実行する場合には、世代番号(プレ記録世代番号)と各記録再生装置に格納されたマスターキーの世代番号の比較処理が記録再生装置において実行され、記録再生装置が自身の記憶手段の格納マスターキーの世代が記録媒体の世代番号(プレ記録世代番号) nより古いものである場合は、図39に示す記録媒体3900に対する記録、及び記録媒体3900からの再生が行えない。

図39に示す記録媒体3900に対するデータの記録及び再生に必要なマスターキーMKの最小の世代はnである。記録再生装置が自身の記憶手段に格納しているマスターキーの世代がnと同一か、より新しい記録再生装置は、記録媒体3900への記録が行える。しかし、記録再生装置が自身の記憶手段に格納しているマスターキーの世代がnより古い場合には、記録媒体3900へのデータの記録は許されず、たとえ不正装置が古いマスターキーを用いて記録を行ったとしても、正しい再生装置はこのデータを再生しない。また、記録媒体3900に正当に記録されるデータは必ずnと同一かより新しい世代のマスターキーに基づいて暗号化されて記録されるため、記録再生装置3900が自身の記憶手段に格納しているマスターキーの世代がnより古い場合には、この記録再生装置は記録媒体のデータを復号できない(再生できない)ことになる。

なお、プレ記録世代情報Generationfnは、記録媒体3900において、その書き換えが不可能な領域(書き換え不可の領域)としての、例えば、リードインエリアに記録されており、これにより、キーテーブル及びプレ記録世代情報Generationfnが不正に書き換えられることを防止するようになっている。

図39に示す記録媒体3900に対するデータの記録は、その記録媒体3900におけるプレ記録世代情報が表す世代以後の世代のマスターキーMKを有していなければ行うことができない(許可されない)ように、装置の設計を行う。したがって、ある世代れを表すプレ記録世代情報Generation#nが記録された記録媒体3900が流通することで、記録媒体3900に対する記録を行う記録装置や、その記録再生が可能な図6の記録再生装置におけるマスターキーの更新が促進され、これにより、前の世代のマスターキーMKを用いている記録装置や記録再生装置が減少していき、その結果、不正なデータの復号が防止される。

すなわち、プレ記録世代情報が記録されていない、例えば前述の図4を用いて説明した記録媒体(光ディスク)150に対しては、上述のように、マスターキーを更新していない記録装置によって、データの記録が可能であり、そのようにしてデータが記録された光ディスク150は、マスターキーを更新していない情報再生装置で再生することができてしまうが、一方、プレ記録世代情報が記録されている図39を用いて説明した記録媒体3900に対しては、プレ記録世代情報が表す世代以後の世代のマスターキーMKを有していなければ、データの記録が許可されない。すなわち、記録媒体3900へのデータの記録を行うには、そこに記録されているプレ記録世代情報が表す世代以後の世代のマスターキーMKが必要となるから、マスターキーを更新していない記録装置によるデータの記録が防止される。

なお、マスターキーの更新処理は、入出力 I / Fや、 I Cカード、モデム等を介してキー更新プロック: KRB (Key Renewal Block) と更新マスターキーをノードキーで暗号化した暗号文を入手し、KRB (Key Renewal Block) の処理により更新されたマスターキーを取得することができる。KRB (Key Renewal Block) の処理可能なデバイスは、前述のようにKRB復号処理可能なノードキー、リーフキーを有するデバイスに限られるので、KRB (Key Renewal Block) 配信時に相互認証を行う必要がなく、正当なデバイスのみが更新されたマスターキーを取得可能となる。

[6. データ処理手段の構成]

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。すなわち、例えば、暗号処理手段650は暗号化/復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図40は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

; ;; プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク4005やROM4003に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、CD-ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク,DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーパブル記録媒体4010に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーパブル記録媒体4010は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体4010からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部4008で受信し、内蔵するハードディスク4005にインストールすることができる。

コンピュータは、CPU(Central Processing Unit)4002を内蔵している。CPU4002には、バス4001を介して、入出力インタフェース4011が接続されており、CPU4002は、入出力インタフェース4010を介して、ユーザによって、キーボードやマウス等で構成される入力部4007が操作されることにより指令が入力されると、それに従って、ROM(Read Only Memory)4003に格納されているプログラムを実行する。

あるいは、CPU4002は、N-ドディスク4005に格納されているプログラム、衛星もしくはネットワークから転送され、通信部4008で受信されて N-ドディスク4005にインストールされたプログラム、又はドライブ4009に装着されたリムーバブル記録媒体4010から読み出されてN-ドディスク4005にインストールされたプログラムを、 $RAM(Random\ Access\ Memory)4004$ にロードして実行する。

これにより、CPU4002は、上述したフローチャートに従った処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU4002は、その処理結果を、必要に応じて、例えば、入出力インタフェース401

1 を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部4006から出力、あるいは、通信部4008から送信、さらには、ハードディスク4005に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理 (例えば、並列処理あるいはオブジェクトによる処理) も含むものである。

また、プログラムは、1つのコンピュータにより処理されるものであってもよいし、複数のコンピュータによって分散処理されるものであってもよい。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであってもよい。

なお、本実施の形態では、コンテンツの暗号化/復号を行うブロックを、1チップの暗号化/復号LSIで構成する例を中心として説明したが、コンテンツの暗号化/復号を行うブロックは、CPUが実行する1つのソフトウェアモジュールとして実現することも可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用をなしうることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

本発明の情報記録再生装置及び方法によれば、記録あるいは再生時に必要な世代の第1のキーを装置が有していない場合に、ユーザに対してキーの更新を促すメッセージを表示することでシステム全体のキーの更新を促進し、不正にデータが複製されることを防止することが可能となる。

加えて、本発明の情報記録再生装置及び方法によれば、記録あるいは再生時に必要な世代の第1のキーを装置が有していない場合に、外部の装置から必要な世代のキーを取得することにより、システム全体のキーの更新を促進し、不正にデ

ータが複製されることを防止することが可能となる。

さらに、本発明の情報記録再生装置及び方法によれば、暗号処理手段において、 装置が格納する世代のキーに基づいて前の世代のキーを生成可能であり、インタ オペラビリティを保ったまま、効果的に不正にデータが複製されることを防止す ることが可能となる。

さらに、本発明の情報記録媒体によれば、暗号化又は復号処型として使用可能なキーの世代を表す世代情報が記録されており、情報記録再生装置は、自身の格納するキーの世代と記録媒体に格納された世代情報との比較処理により、記録再生の可否が決定される。したがって、例えば無効となった過去のキーによる不正データの複製を防止することが可能となる。

さらに、本発明のキー更新端末装置及びキー更新方法によれば、記録再生器とは別体として構成されるキー更新端末装置を介する更新キーの入手が可能となり、例えば、同一カテゴリに属する他の機器のデバイスキーの欝呈によってマスターキーの更新が必要となった機器が、キー更新端末を介してキー発行機関と通信路を確立、もしくは、キー更新端末から直接、マスターキーを入手することが可能となり、同一のカテゴリに属する端末中の個々の端末に対して個別の対応が可能となる。

さらに、本発明の情報記録再生装置及び方法によれば、ツリー (木) 構造の鍵配布構成により、マスターキーの更新データを更新ブロック (KRB) とともに送信する構成としたので、鍵更新の必要なデバイスにのみ復号可能な構成とした伝送又は配布が可能となり、メッセージ量を小さく抑えることができる。さらに、ツリー構造によって規定される特定のグループにのみ復号可能な鍵を配布可能であり、グループに属さない他のデバイスには復号できない構成とすることが可能であり、キー配信又は配布の安全性が確保される。

請求の範囲

1. 記録媒体に情報を記録する情報記録装置において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく 暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処型 手段と、

前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、警告出力を実行するユーザインタフェースと、

を有することを特徴とする情報記録装置。

- 2. 前記装置格納世代管理暗号化キーは、複数の情報記録装置に共通に格納されたマスターキーであることを特徴とする請求の範囲第1項に記載の情報記録装置。
- 3. 前記暗号処理手段は、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含むことを特徴とする請求の範囲第1項に記載の情報記録装置。

4. 前記暗号処理手段は、

前記装置格納世代管理暗号化キーの世代情報よりも古い世代情報の世代管理暗号化キーを、前記装置格納世代管理暗号化キーに基づいて生成するキー生成手段を有する構成であることを特徴とする請求の範囲第1項に記載の情報記録装置。

5. 前記暗号処理手段は、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号 化キーに更新処理を実行する更新手段を含み、

前記更新手段は、

e Professional Company of the Compan

暗号化処理の施された更新用世代管理暗号化キーについての復号処理を、前記情報記録装置に格納されたデバイスキーに基づいて実行し、更新された世代管理暗号化キーを生成する構成を有することを特徴とする請求の範囲第1項に記載の情報記録装置。

6. 前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理暗号化キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理暗号化キーについての復号処理を実行する構成であることを特徴とする請求の範囲第5項に記載の情報記録装置。

- 7. 前記デバイスキーは、情報記録装置をカテゴリ区分し、共通のカテゴリに属する情報記録装置に共通のキーとした構成であることを特徴とする請求の範囲第5項に記載の情報記録装置。
- 8. 前記デバイスキーは、情報記録装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする請求の範囲第5項に記載の情報記録装置。
- 9. 前記情報記録装置は、

複数の異なる情報記録装置をリーフとした階層ッリー構造を構成する各ノード に固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲 第1項に記載の情報記録装置。

- 10. 前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第9項に記載の情報記録装置。
- 11. 前記ノードキーは、更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック (KRB) を更新対象となるリーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを 受領し、

キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする請求の範囲第9項に記載の情報記録装置。

12. 前記キー更新ブロック (KRB) は、記録媒体に格納され、 前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする請求の範囲第9項に記載の情報記録装置。

13. 前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求の範囲第9項に記載の情報記録装置。

14. 記録媒体に情報を記録する情報記録装置において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、

前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得手段と、

を有することを特徴とする情報記録装置。

15. 前記キー取得手段は、

ネットワークを介するデータ受信の実行可能な通信インタフェースを含むこと

を特徴とする請求の範囲第14項に記載の情報記録装置。

16. 前記キー取得手段は、

電話回線を介するデータ受信の実行可能な通信モデムを含むことを特徴とする 請求の範囲第14項に記載の情報記録装置。

17. 前記キー取得手段は、

I Cカードを介するデータ受信の実行可能な I / Cカードインタフェースを含むことを特徴とする請求の範囲第14項に記載の情報記録装置。

18. 前記暗号処理手段は、

前記キー取得手段によるキー取得実行の際に、キー提供手段との相互認証処理 を実行する構成を有し、

前記キー取得手段は、前記相互認証処理の成立を条件として前記世代管理暗号 化キーの取得を実行する構成であることを特徴とする請求の範囲第14項に記載 の情報記録装置。

- 19. 前記装置格納世代管理暗号化キーは、複数の情報記録装置に共通に格納されたマスターキーであることを特徴とする請求の範囲第14項に記載の情報記録装置。
- 20. 前記暗号処理手段は、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含むことを特徴とする請求の範囲第14項に記載の情報記録装置。

21. 前記暗号処理手段は、

前記暗号処理手段は、

22.

前記装置格納世代管理暗号化キーの世代情報よりも古い世代情報の世代管理暗号化キーを、前記装置格納世代管理暗号化キーに基づいて生成するキー生成手段を有する構成であることを特徴とする請求の範囲第14項に記載の情報記録装置。

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含み、

前記更新手段は、

暗号化処理の施された更新用世代管理暗号化キーについての復号処理を、前記情報記録装置に格納されたデバイスキーに基づいて実行し、更新された世代管理暗号化キーを生成する構成を有することを特徴とする請求の範囲第14項に記載の情報記録装置。

23. 前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理暗号化キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理暗号化キーについての復号処理を実行する構成であることを特徴とする請求の範囲第22項に記載の情報記録装置。

- 24. 前記デバイスキーは、情報記録装置をカテゴリ区分し、共通のカテゴリに属する情報記録装置に共通のキーとした構成であることを特徴とする請求の範囲第22項に記載の情報記録装置。
- 25. 前記デバイスキーは、情報記録装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする請求の範囲第22項に記載の情報記録装置。
- 26. 前記情報記録装置は、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノード に固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲 第14項に記載の情報記録装置。

- 27. 前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第26項に記載の情報記録装置。
- 28. 前記ノードキーは更新可能なキーとして構成され、更新処理に際しては 更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを 含むキーにより暗号化したキー更新ブロック (KRB) を更新対象となるリーフ の情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを 受領し、

キー更新プロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする請求の範囲第26項に記載の情報記録装置。

29. 前記キー更新ブロック (KRB) は、記録媒体に格納され、 前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする請求の範囲第26項に記載の情報記録 装置。

30. 前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求の範囲第26項に記載の情報記録装置。

31. 記録媒体に情報を記録する情報記録装置において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理 手段と、

前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーを取得するためのキー更新端末を接続するキー更新端末接続インタフェースと、

を有することを特徴とする情報記録装置。

32. 前記情報記録装置は、

前記キー更新端末からの前記世代管理暗号化キー取得実行の際に、前記キー更 新端末との相互認証処理を実行する構成を有し、

前記情報記録装置は、前記相互認証処理の成立を条件として前記世代管理暗号 化キーの取得を実行する構成であることを特徴とする請求の範囲第31項に記載 の情報記録装置。

33. 前記情報記録装置は、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノード に固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第31項に記載の情報記録装置。

- 34. 前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第33項に記載の情報記録装置。
- 35. 前記ノードキーは更新可能なキーとして構成され、更新処理に際しては 更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを 含むキーにより暗号化したキー更新ブロック (KRB) を更新対象となるリーフ の情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、

キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする請求の範囲第33項に記載の情報記録装置。

36. 前記キー更新ブロック (KRB) は、記録媒体に格納され、 前記暗号処理手段は、

前記記録媒体から読み出されたキー更新プロック (KRB) についての暗号処理を実行する構成であることを特徴とする請求の範囲第33項に記載の情報記録

装置。

37. 前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求の範囲第33項に記載の情報記録装置。

38. 記録媒体から情報を再生する情報再生装置において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復 号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処 理手段と、

前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報との比較において、前記記録時世代情報が前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に警告出力を実行するユーザインタフェースと、

を有することを特徴とする情報再生装置。

39. 前記暗号処理手段は、

前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報との比較処理において前記プレ世代情報が前記記録時世代情報よりも新しいものである場合に復号処理を実行しない構成としたことを特徴とする請求の範囲第38項に記載の情報再生装置。

- 40. 前記装置格納世代管理復号キーは、複数の情報再生装置に共通に格納されたマスターキーであることを特徴とする請求の範囲第38項に記載の情報再生装置。
- 41. 前記暗号処型手段は、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復

号キーに更新処理を実行する更新手段を含むことを特徴とする請求の範囲第38 項に記載の情報再生装置。

42. 前記暗号処理手段は、

前記装置格納世代管理復号キーの世代情報よりも古い世代情報の世代管理復号キーを、前記装置格納世代管理復号キーに基づいて生成するキー生成手段を有する構成であることを特徴とする請求の範囲第38項に記載の情報再生装置。

43. 前記暗号処理手段は、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復 号キーに更新処理を実行する更新手段を含み、

前記更新手段は、

暗号化処理の施された更新用世代管理復号キーについての復号処理を、前記情報再生装置に格納されたデバイスキーに基づいて実行し、更新された世代管理復号キーを生成する構成を有することを特徴とする請求の範囲第38項に記載の情報再生装置。

44. 前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理復号キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理復号キーについての復号処理を実行する構成であることを特徴とする請求の範囲第43項に記載の情報再生装置。

- 45. 前記デバイスキーは、情報再生装置をカテゴリ区分し、共通のカテゴリに属する情報再生装置に共通のキーとした構成であることを特徴とする請求の範囲第43項に記載の情報再生装置。
- 46. 前記デバイスキーは、情報再生装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする請求の範囲第43項に記載の情報再生装置。

47. 前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノード

に固有のノードキーと各情報再生装置固有のリーフキーとを保有し、

前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第38項に記載の情報再生装置。

- 48. 前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする請求の範囲第47項に記載の情報再生装置。
- 49. 前記ノードキーは更新可能なキーとして構成され、更新処理に際しては 更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを 含むキーにより暗号化したキー更新ブロック (KRB) を更新対象となるリーフ の情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、

キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする請求の範囲第47項に記載の情報再生装置。

50. 前記キー更新ブロック (KRB) は、記録媒体に格納され、前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする請求の範囲第47項に記載の情報再生 装置。

51. 前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする請求の範囲第47項に記載の情報再生装置。

52. 記録媒体から情報を再生する情報再生装置において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復 号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処 理手段と、

前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得手段と、

を有することを特徴とする情報再生装置。

53. 前記情報再生装置は、

前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報との比較処理を実行して該比較処理において前記プレ世代情報が前記記録時世代情報よりも新しいものである場合に再生処理を実行しない構成としたことを特徴とする請求の範囲第52項に記載の情報再生装置。

54. 前記キー取得手段は、

ネットワークを介するデータ受信の実行可能な通信インタフェースを含むことを特徴とする請求の範囲第52項に記載の情報再生装置。

55. 前記キー取得手段は、

電話回線を介するデータ受信の実行可能な通信モデムを含むことを特徴とする 請求の範囲第52項に記載の情報再生装置。

56. 前記キー取得手段は、

I Cカードを介するデータ受信の実行可能な I / Cカードインタフェースを含むことを特徴とする請求の範囲第52項に記載の情報再生装置。

57. 前記暗号処理手段は、

前記キー取得手段によるキー取得実行の際に、キー提供手段との相互認証処理 を実行する構成を有し、

前記キー取得手段は、前記相互認証処理の成立を条件として前記世代管理復号

キーの取得を実行する構成であることを特徴とする請求の範囲第52項に記載の情報再生装置。

58. 前記装置格納世代管理復号キーは、複数の情報再生装置に共通に格納されたマスターキーであることを特徴とする請求の範囲第52項に記載の情報再生 装置。

59. 前記暗号処理手段は、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含むことを特徴とする請求の範囲第52項に記載の情報再生装置。

60. 前記暗号処理手段は、

前記装置格納世代管理復号キーの世代情報よりも古い世代情報の世代管理復号キーを、前記装置格納世代管理復号キーに基づいて生成するキー生成手段を有する構成であることを特徴とする請求の範囲第52項に記載の情報再生装置。

61. 前記暗号処理手段は、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復 号キーに更新処理を実行する更新手段を含み、

前記更新手段は、

暗号化処理の施された更新用世代管理復号キーについての復号処理を、前記情報再生装置に格納されたデバイスキーに基づいて実行し、更新された世代管理復号キーを生成する構成を有することを特徴とする請求の範囲第52項に記載の情報再生装置。

62. 前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理復号キーと、暗号復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理復号キーについての復号処理を実行する構成であることを特徴とする請求の範囲第61項に記載の情報再生装置。

- 63. 前記デバイスキーは、情報再生装置をカテゴリ区分し、共通のカテゴリに属する情報再生装置に共通のキーとした構成であることを特徴とする請求の範囲第61項に記載の情報再生装置。
- 64. 前記デバイスキーは、情報再生装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする請求の範囲第61項に記載の情報再生装置。
- 65. 前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、

前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第52項に記載の情報再生装置。

- 66. 前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする請求の範囲第65項に記載の情報再生装置。
- 67. 前記ノードキーは更新可能なキーとして構成され、更新処理に際しては 更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを 含むキーにより暗号化したキー更新ブロック (KRB) を更新対象となるリーフ の情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、

キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする請求の範囲第65項に記載の情報再生装置。

68. 前記キー更新ブロック (KRB) は、記録媒体に格納され、 前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする請求の範囲第65項に記載の情報再生

装置。

69. 前記世代管理復号キーは、更新情報としての世代番号が対応付けられた 構成であり、

前記暗号処理部は、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする請求の範囲第65項に記載の情報再生装置。

70. 記録媒体から情報を再生する情報再生装置において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復 号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処 理手段と、

前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーを取得するためのキー更新端末を接続するキー更新端末接続インタフェースと、

を有することを特徴とする情報再生装置。

71. 前記情報再生装置は、

前記キー更新端末からの前記世代管理復号キー取得実行の際に、前記キー更新端末との相互認証処理を実行する構成を有し、

前記情報再生装置は、前記相互認証処理の成立を条件として前記世代管理復号 キーの取得を実行する構成であることを特徴とする請求の範囲第70項に記載の 情報再生装置。

72. 前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、

前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれ

かを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第70項に記載の情報再生装置。

- 73. 前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする請求の範囲第72項に記載の情報再生装置。
- 74. 前記ノードキーは更新可能なキーとして構成され、更新処理に際しては 更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを 含むキーにより暗号化したキー更新ブロック (KRB) を更新対象となるリーフ の情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処型した前記世代管理復号キーの更新データを受領し、

キー更新ブロック (KRB) の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする請求の範囲第72項に記載の情報再生装置。

75. 前記キー更新ブロック (KRB) は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック (KRB) についての暗号処理を実行する構成であることを特徴とする請求の範囲第72項に記載の情報再生装置。

76. 前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする請求の範囲第72項に記載の情報再生装置。

77. 記録媒体に情報を記録する情報記録方法において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく

暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理 ステップを有し、

さらに、

情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、警告出力を実行する警告出力ステップと、

を有することを特徴とする情報記録方法。

78. 記録媒体に情報を記録する情報記録方法において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく 暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理 ステップを有し、

さらに、

情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得ステップと、

を有することを特徴とする情報記録方法。

79. 前記情報記録方法において、

前記キー取得ステップは、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを 用いて前記世代管理暗号化キーの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された世代管理暗号化キーに基づいて前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を含むことを特徴とする請求の範囲第78項に記載の情報記録方法。

- 80. 前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第79項に記載の情報記録方法。
- 81. 前記情報記録方法において、

前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報記録装置に配布する構成であり、

前記更新ステップは、

前記キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを算出する更新データ取得ステップと、

を含むことを特徴とする請求の範囲第79項に記載の情報記録方法。

82. 前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理ステップは、さらに、

前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする請求の範囲第79項に記載の情報記録方法。

83. 記録媒体から情報を再生する情報再生方法において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復 号処理によって前記記録媒体の格納情報の復号処理を実行する復号処理ステップ を有し、

さらに、

情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、 前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報 とを比較するステップと、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、警告出力を実行する警告出力ステップと、

を有することを特徴とする情報再生方法。

84. 記録媒体から情報を再生する情報再生方法において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復 号処理によって前記記録媒体の格納情報の復号処理を実行する復号処理ステップ を有し、

さらに、

情報記録再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理 復号キーの取得を実行するキー取得ステップと、

を有することを特徴とする情報再生方法。

85. 前記情報再生方法において、

前記キー取得ステップは、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを 用いて記録媒体に格納された暗号データの復号処理を実行する世代管理復号キー の更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された世代管理復号キーに基づいて前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、

を含むことを特徴とする請求の範囲第84項に記載の情報再生方法。

- 86. 前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする請求の範囲第85項に記載の情報再生方法。
- 87. 前記情報再生方法において、

前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック(KRB)を更新対象となるリーフの情報再生装置に配布する構成であり、

前記更新ステップは、

前記キー更新ブロック(KRB)の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを算出 する更新データ取得ステップと、

を含むことを特徴とする請求の範囲第85項に記載の情報再生方法。

88. 前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、

前記復号処理ステップは、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して実行することを特徴とする請求の範囲第85項に記載の情報再生方法。

89. 情報の記録可能な情報記録媒体であって、

該情報記録媒体に対する暗号化データの書き込みに使用可能な暗号化キー、又は該情報記録媒体の格納データの復号処理に使用可能な復号キーとして許容されるキーの世代情報としてのプレ世代情報を格納したことを特徴とする情報記録媒体。

- 90. 前記プレ世代情報は、前記情報記録媒体における書き換え不可領域に記録されていることを特徴とする請求の範囲第89項に記載の情報記録媒体。
- 91. 世代毎に更新され、異なるキーとして設定される世代管理キーに基づく 処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対 する更新世代管理キーの提供を行うキー更新端末装置であり、

前記情報記録又は再生装置に接続可能なインタフェースと、

外部との通信を実行する通信手段と、

前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理、該装置固有識別子の前記通信手段を介する送信処理、前記通信手段を介する更新世代管理キーの受信処理、及び前記インタフェースを介する前記情

報記録又は再生装置に対する更新世代管理キーの転送処理の各制御を実行する制 御手段と、

を有することを特徴とするキー更新端末装置。

92. 世代毎に更新され、異なるキーとして設定される世代管理キーに基づく 処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取ら れる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対 する更新世代管理キーの提供を行うキー更新端末装置であり、

前記情報記録又は再生装置に接続可能なインタフェースと、

装置固有の暗号化鍵で暗号化された世代管理キーを、前記情報記録又は再生装置の装置固有識別子に対応付けたキーテーブルを格納した記憶手段と、

前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理、該装置固有識別子に基づく前記記憶手段からの該装置固有識別子に対応する暗号化世代管理キーの取得処理、及び前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理の各制御を実行する制御手段と、

を有することを特徴とするキー更新端末装置。

93. 前記キー更新端末装置は、

前記情報記録又は再生装置との相互認証処理を実行する構成を有し、

前記キー更新端末装置は、前記相互認証処理の成立を条件として前記世代管理 キーの前記情報記録又は再生装置に対する提供処理を実行する構成であることを 特徴とする請求の範囲第92項に記載のキー更新端末装置。

94. 世代毎に更新され、異なるキーとして設定される世代管理キーに基づく 処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取ら れる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対 する更新世代管理キーの提供を行う世代管理キー更新方法であり、

前記情報記録又は再生装置に接続可能なインタフェースと、外部との通信を実行する通信手段とを有するキー更新端末装置を前記情報記録又は再生装置に接続するステップと、

前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子

の取得処理ステップと、

装置固有識別子の前記通信手段を介する送信処理ステップと、

前記通信手段を介する更新世代管理キーの受信処理ステップと、

前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理ステップと、

を有することを特徴とする世代管理キー更新方法。

95. 世代毎に更新され、異なるキーとして設定される世代管理キーに基づく 処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対 する更新世代管理キーの提供を行う世代管理キー更新方法であり、

前記情報記録又は再生装置に接続可能なインタフェースと、装置固有の暗号化 鍵で暗号化された世代管理キーを、前記情報記録又は再生装置の装置固有識別子 に対応付けたキーテーブルを格納した記憶手段とを有するキー更新端末装置を前 記情報記録又は再生装置に接続するステップと、

前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理ステップと、

装置固有識別子に基づく前記記憶手段からの該装置固有識別子に対応する暗号 化世代管理キーの取得処理ステップと、

前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理ステップと、

を有することを特徴とする世代管理キー更新方法。

96. 前記世代管理キー更新方法において、さらに、

前記情報記録又は再生装置との相互認証処理を実行するステップを有し、

前記相互認証処理の成立を条件として前記世代管理キーの前記情報記録又は再 生装置に対する提供処理を実行することを特徴とする請求の範囲第95項に記載 の世代管理キー更新方法。

97. 記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で 実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、 前記コンピュータ・プログラムは、 情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、

さらに、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、

警告出力ステップ、

あるいは前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの 取得を実行するキー取得ステップと、

の少なくともいずれかを実行するステップ

を有することを特徴とするプログラム提供媒体。

98. 前記コンピュータ・プログラムは、さらに、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する世代管理暗号化キーの更新処理を実行する更新ステップを含むことを特徴とする請求の範囲第97項に記載のプログラム提供媒体。

99. 記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、 前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報 とを比較するステップと、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復 号処理によって前記記録媒体からの格納情報の復号処理を実行する復号処理ステ ップを有し、 さらに、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、

警告出力ステップ、

あるいは前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得ステップと、

の少なくともいずれかを実行するステップ

を有することを特徴とするプログラム提供媒体。

100. 前記コンピュータ・プログラムは、さらに、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する世代管理復号キーの更新処理を実行する更新ステップを含むことを特徴とする請求の範囲第99項に記載のプログラム提供媒体。

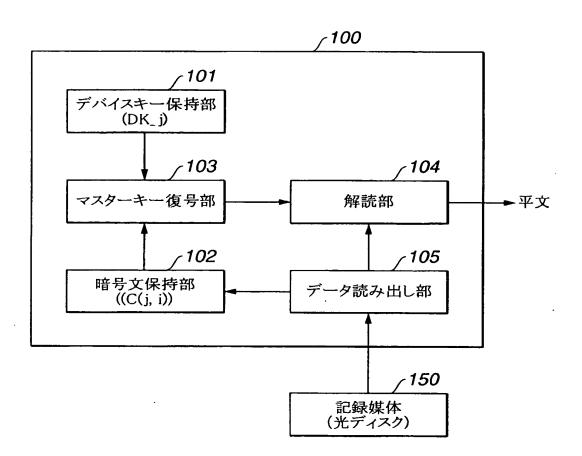


FIG.1

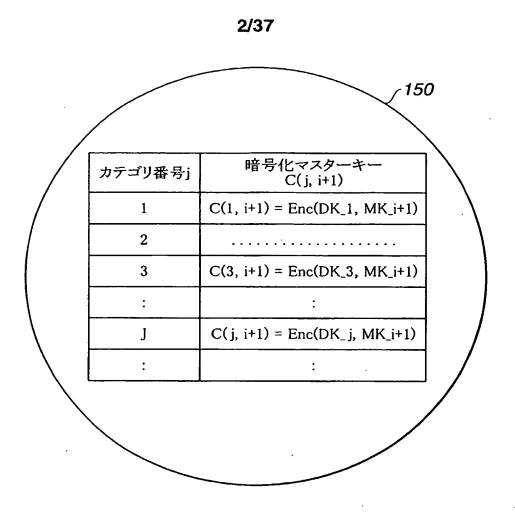


FIG.2

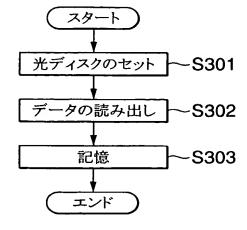


FIG.3

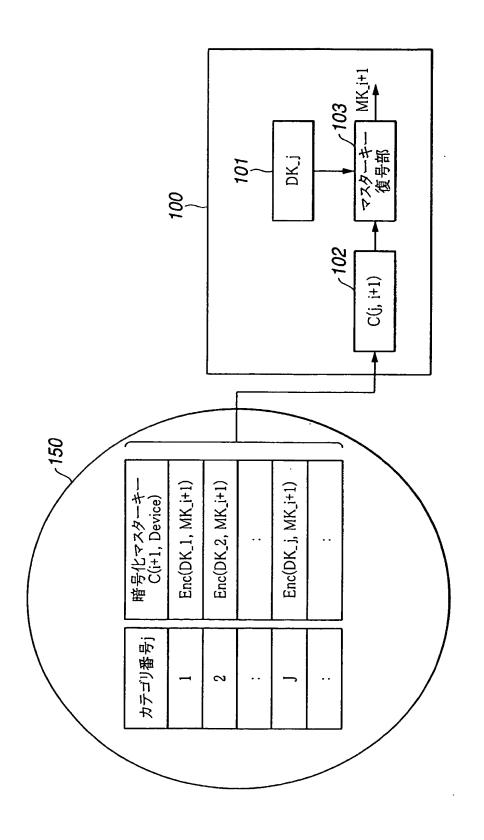


FIG.4

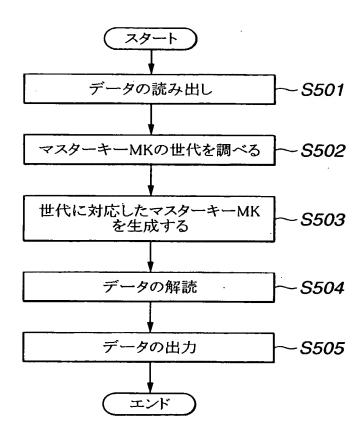


FIG.5

5/37

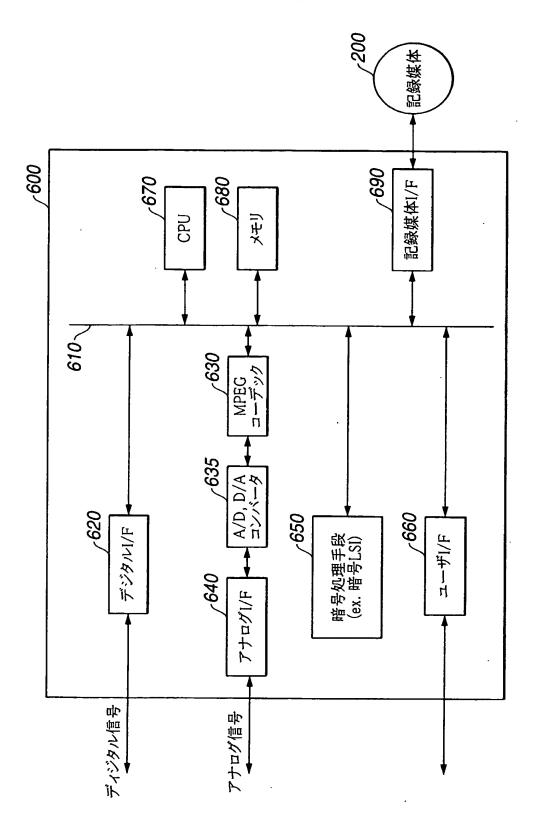


FIG.6

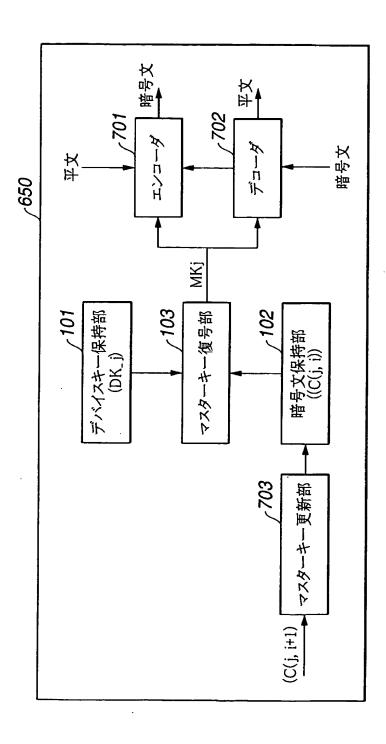


FIG.7

7/37

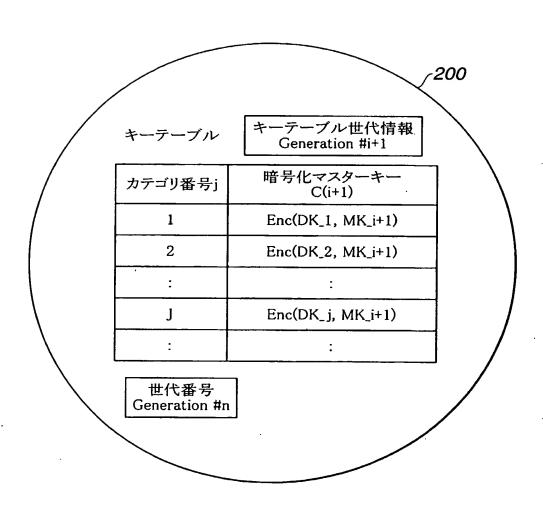


FIG.8

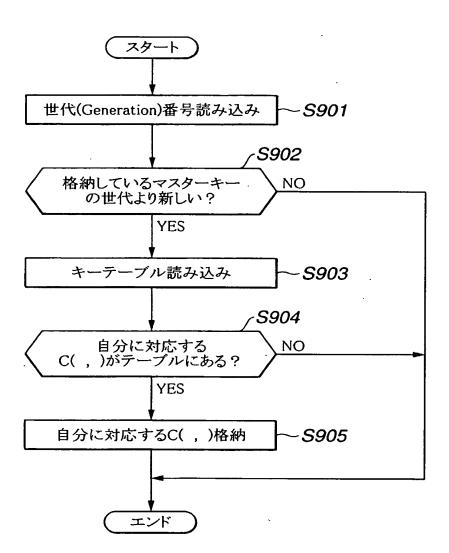


FIG.9

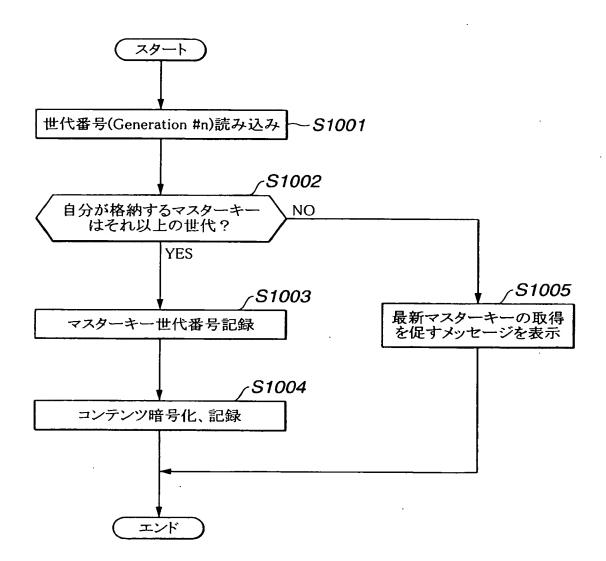


FIG.10

10/37

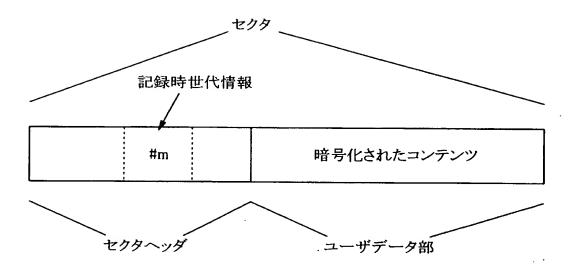


FIG.11

11/37

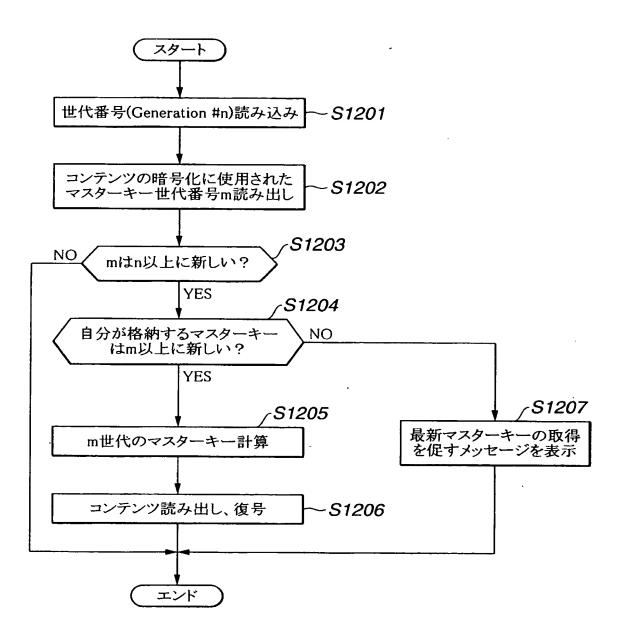


FIG.12

12/37

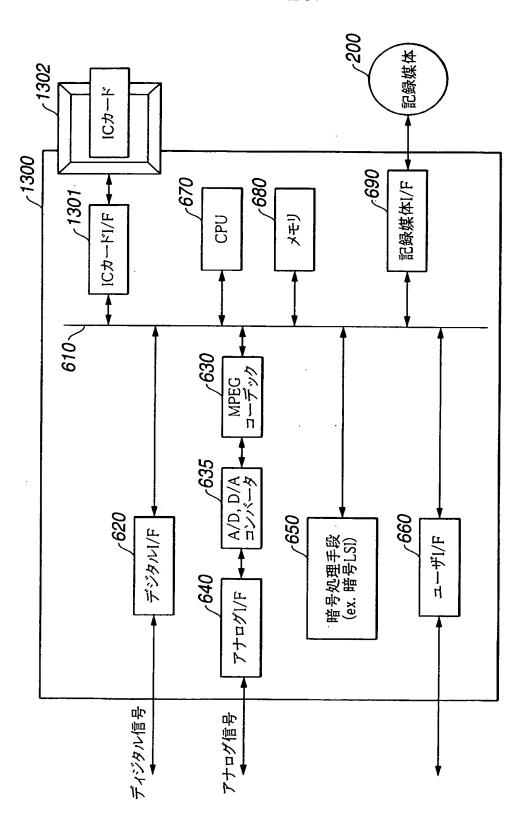


FIG. 13

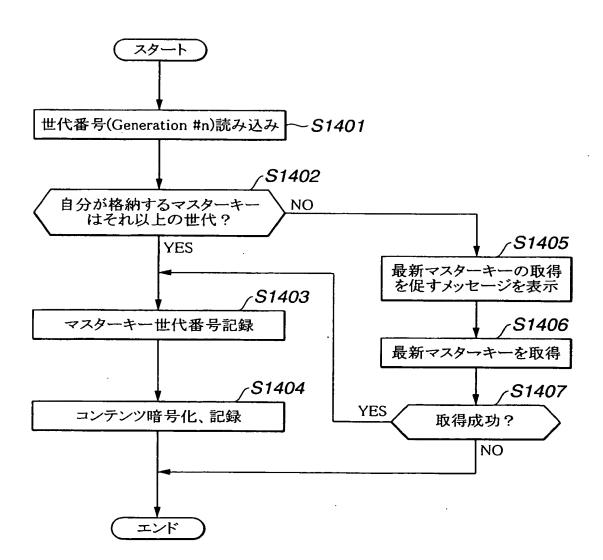


FIG.14

14/37

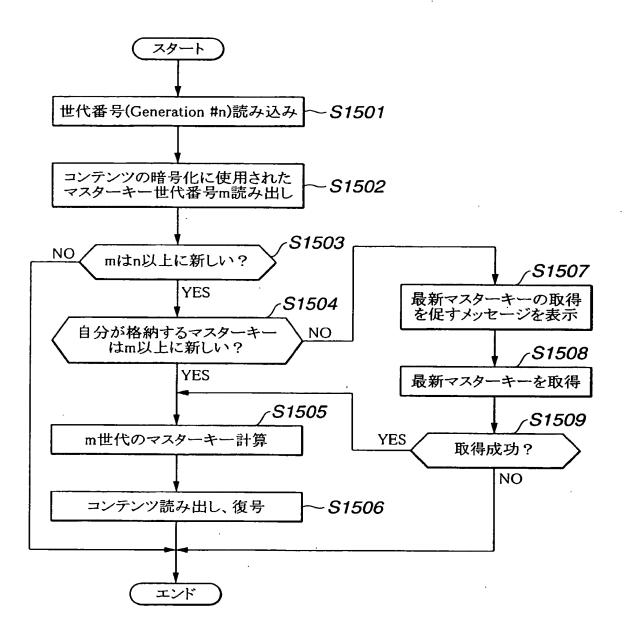


FIG.15

15/37

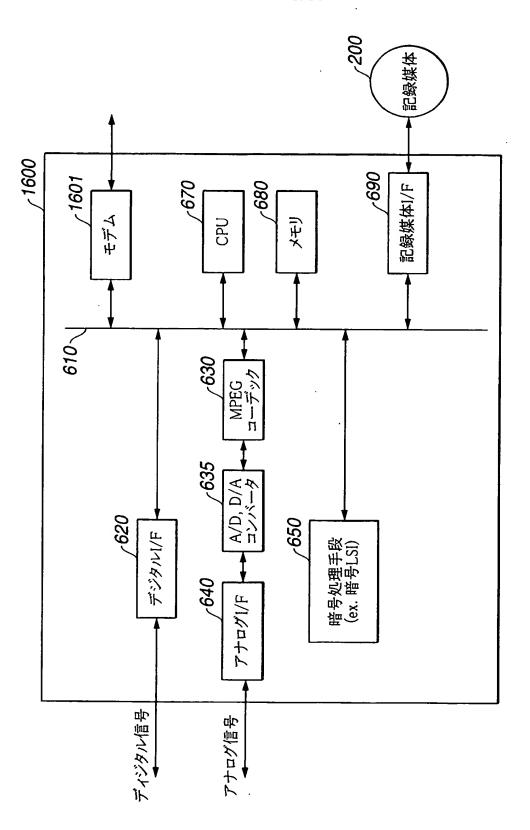


FIG. 16

16/37

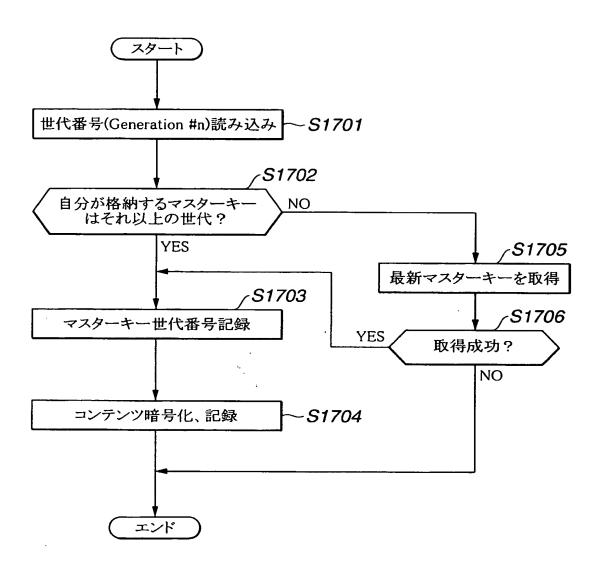


FIG.17

17/37

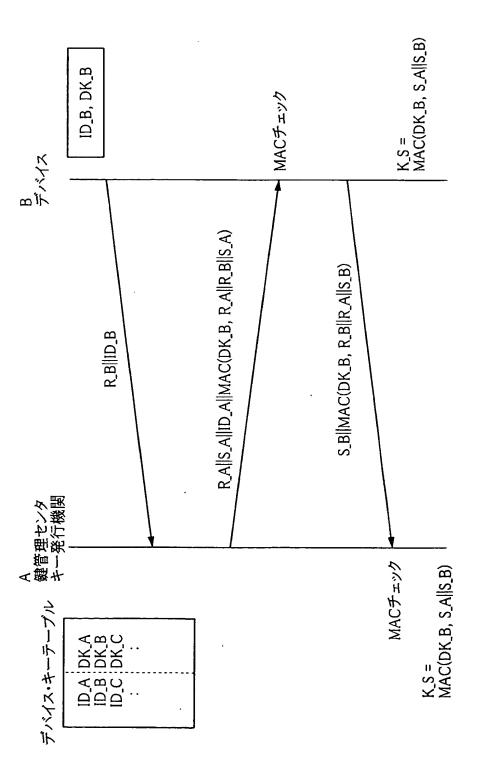
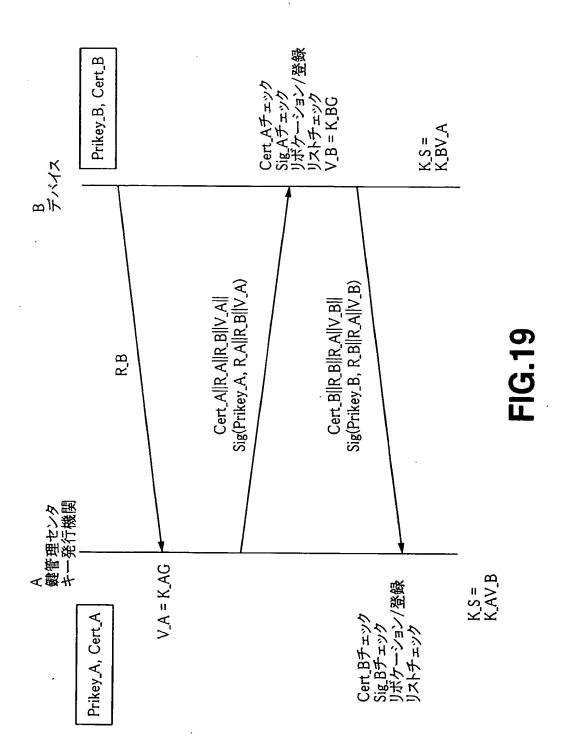


FIG.18

18/37



BのID(ID_B)

Bの公開鍵(Pubkey_B)

上記の全フィールドに対するセンタのデジタル署名

FIG.20

バージョンナンバ	
リボークされる機器のID	
:	
センタのデジタル署名	

FIG.21

バージョンナンバ
登録される機器のID
:
·.
センタのデジタル署名

FIG.22

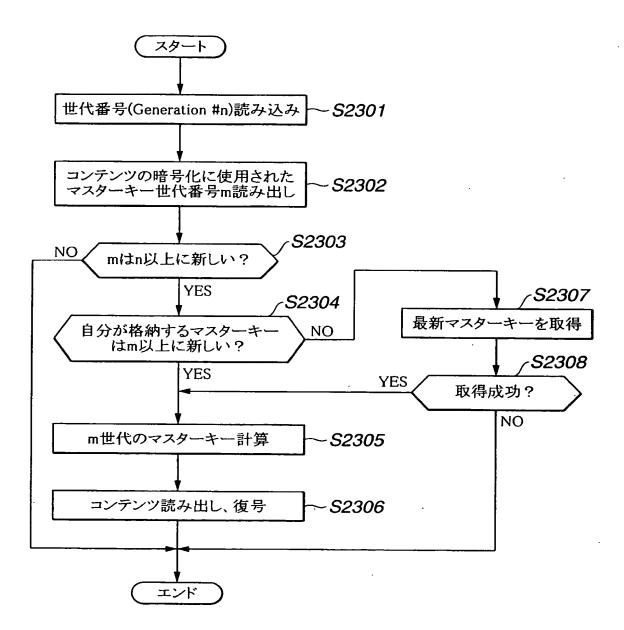


FIG.23

21/37

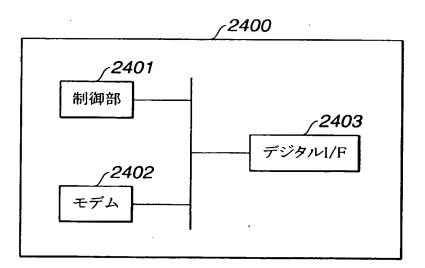
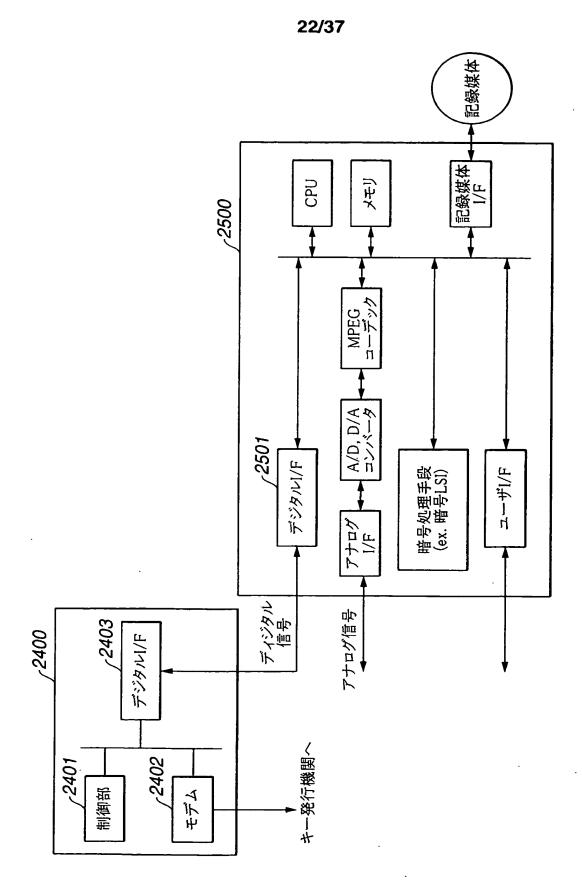


FIG.24

FIG.25



23/37

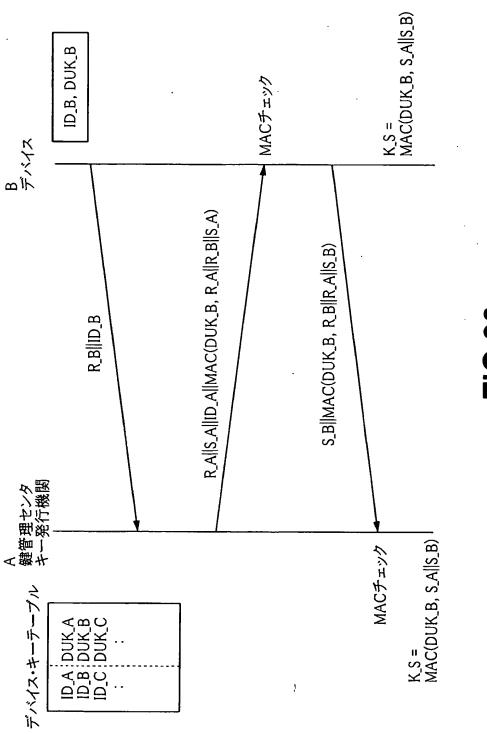
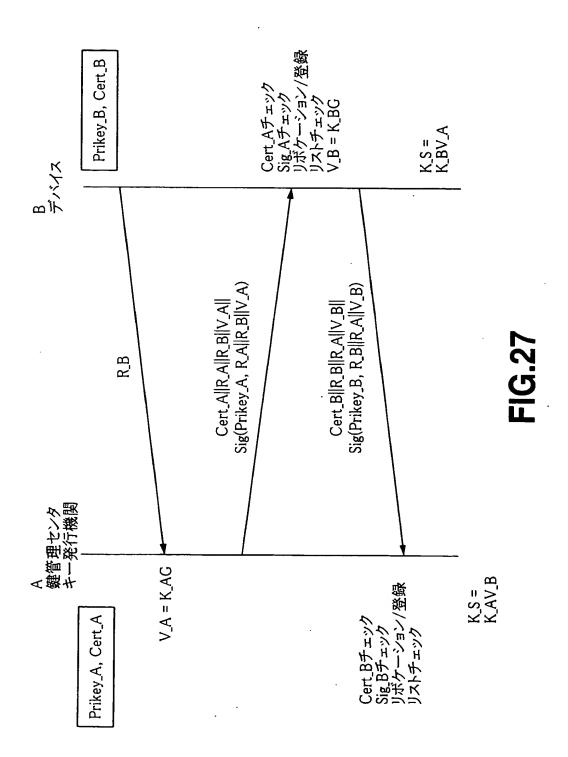


FIG.26

24/37



世代番号#n		
装置固有識別番号(機器ID)	暗号化マスターキー	
1	Enc(DUK_1, MK_n)	
2	Enc(DUK_2, MK_n)	
:	:	
L	· Enc(DUK_L, MK_n)	

FIG.28



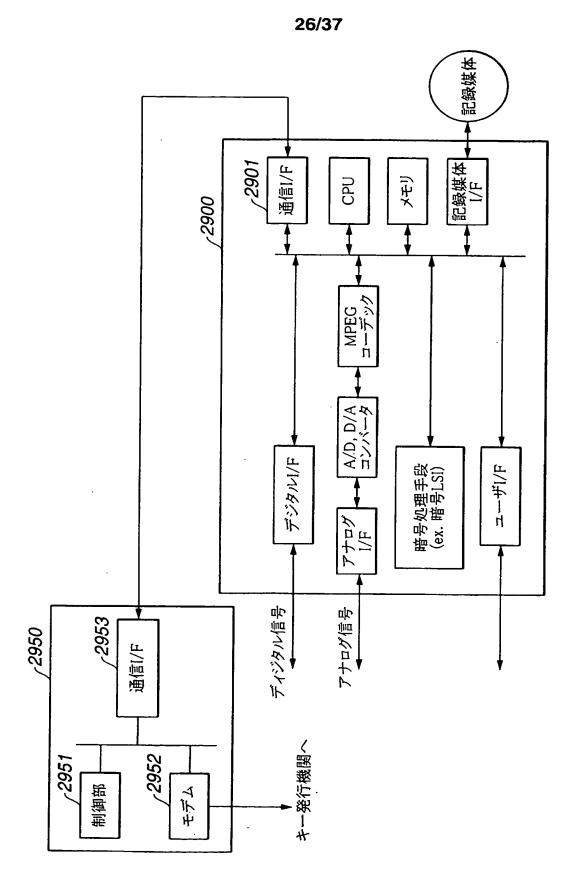
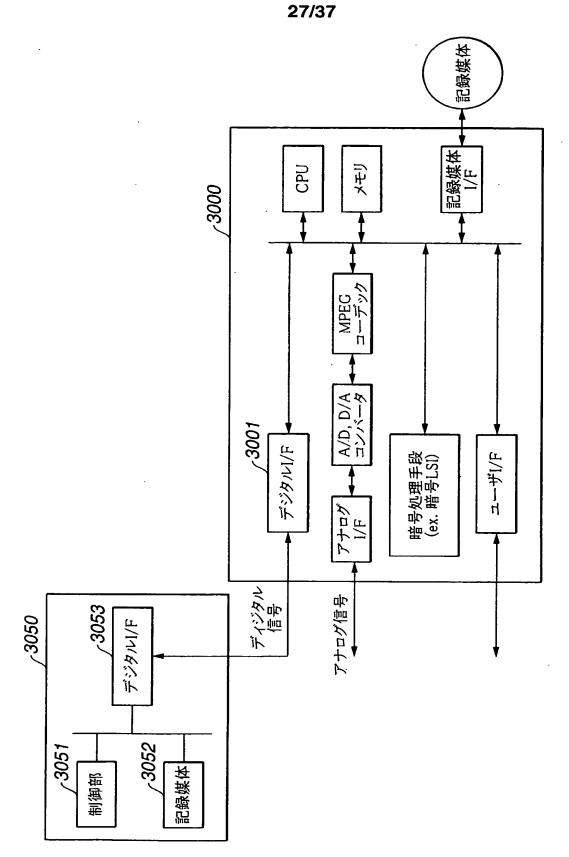


FIG.30



3150

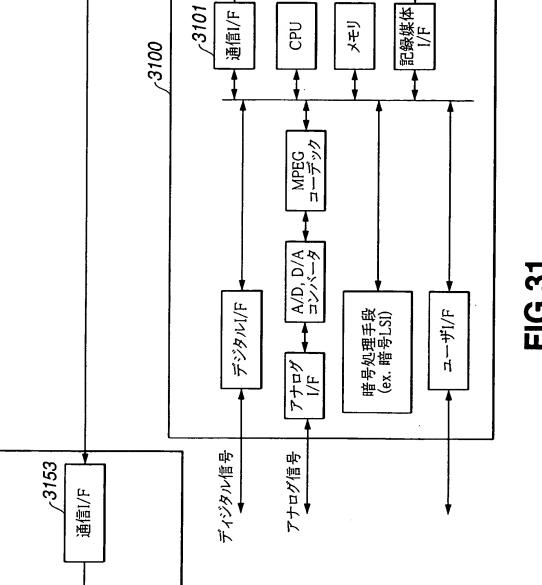
-3151

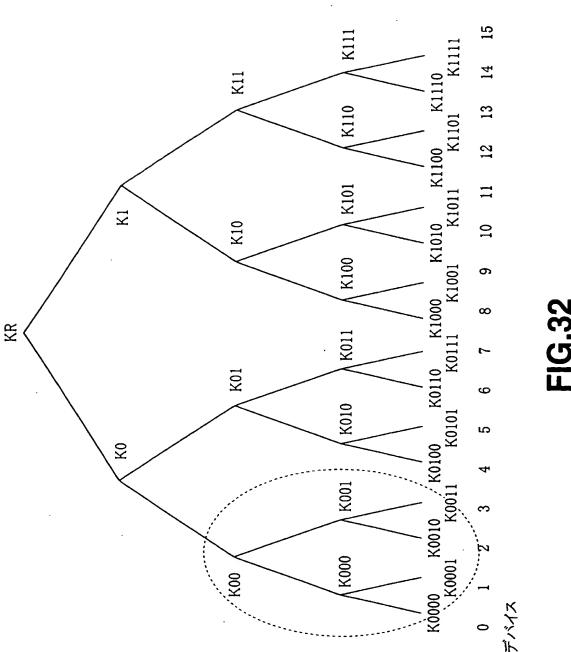
制御部

3152

記録媒体

記錄媒体





世代(Generation):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.33A

世代(Generation	世代(Generation): t	
インデックス	暗号化キー	
000	Enc(K000, K(t)00)	
001	Enc(K(t)001, K(t)00)	
0010	Enc(K0010, K(t)001)	

FIG.33B

31/37

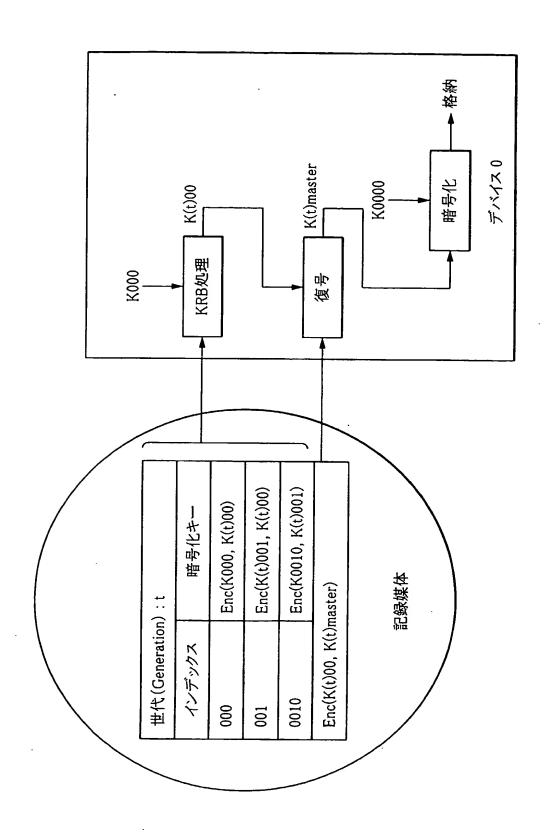


FIG.34

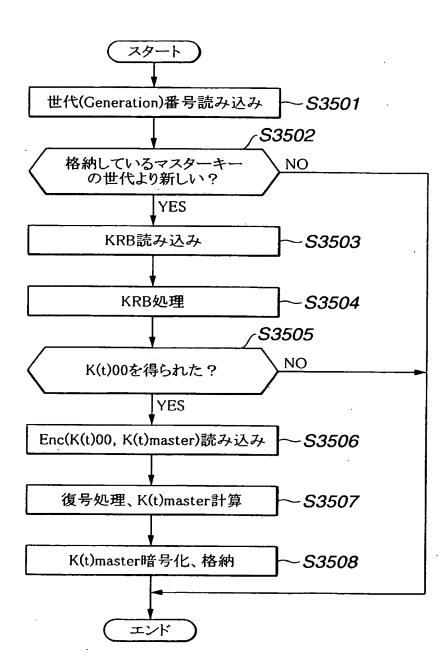


FIG.35

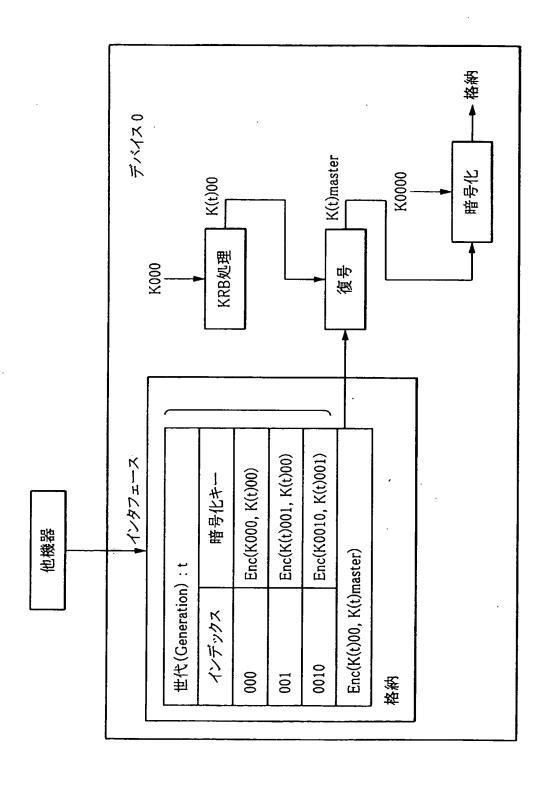


FIG.36

34/37

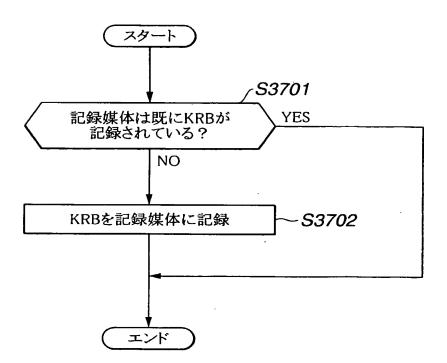


FIG.37

35/37

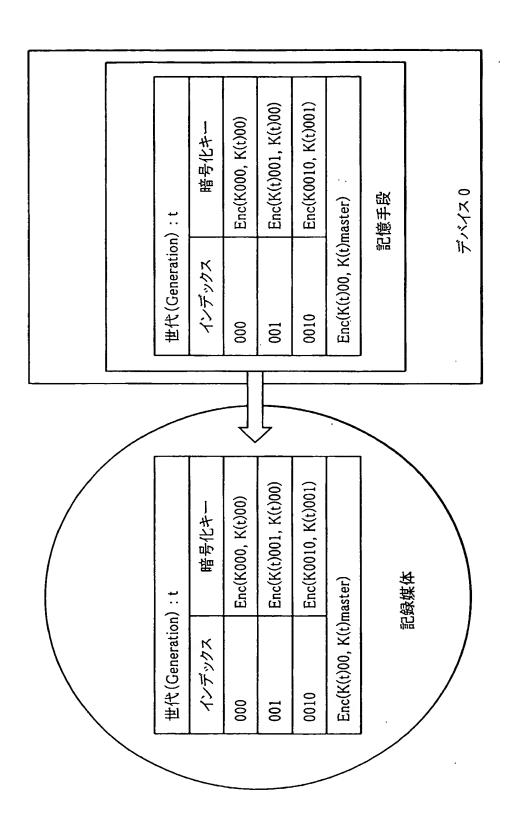


FIG.38

36/37

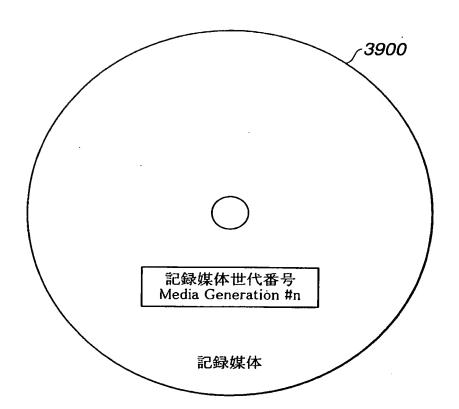
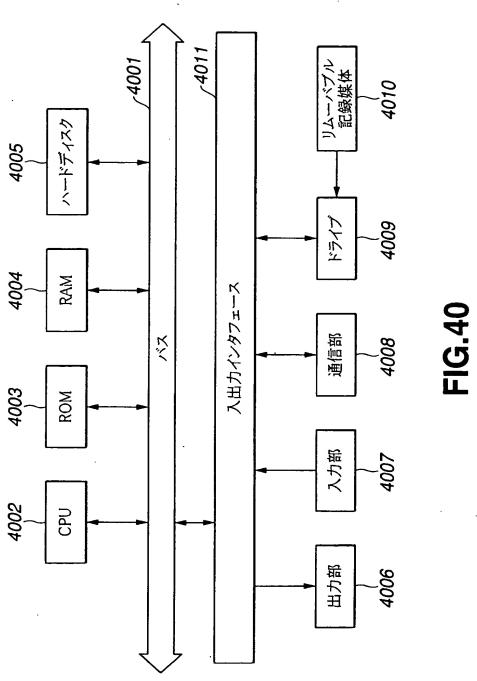


FIG.39

37/37





Internation application No.
PCT/JP01/03004

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl ⁷ H04L9/00, G11B20/10, G11B20/12			
According to International Patent Classification (IPC) or to both	national classification and IPC		
B. FIELDS SEARCHED			
Minimum documentation searched (classification system follow Int.Cl ⁷ H04L9/00, G11B20/10, G11			
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001			
Electronic data base consulted during the international search (r WPI, JICST DATABASE ON SCIENCE AN	name of data base and, where practicable, sea D TECHNOLOGY key, tree, g	rch terms used) eneration, DVD	
C. DOCUMENTS CONSIDERED TO BE RELEVANT			
Category* Citation of document, with indication, when	e appropriate, of the relevant passages	Relevant to claim No.	
X JP, 10-3256, A (Sony Corporat	cion),	89,90	
06 January, 1998 (06.01.98), A Par. Nos. [0037] to [0048]	(Family: none)	1-88,91-100	
12 February, 1999 (12.02.99), Full text	JP, 11-39795, A (Toshiba Corporation), 12 February, 1999 (12.02.99), Full text & KR, 99013756, A & CN, 1208925, A		
	JP, 10-293726, A (Toshiba Corporation), 1-100 04 November, 1998 (04.11.98),		
	JP, 11-250571, A (Matsushita Electric Ind. Co., Ltd.), 1-100 17 September, 1999 (17.09.99), Full text (Family: none)		
17 September, 1999 (17.09.99)	A JP, 11-250570, A (Matsushita Electric Ind. Co., Ltd.), 1-100 17 September, 1999 (17.09.99), column 13, line 17 to column 16, line 32 (Family: none)		
A JP, 11-126425, A (Sony Corpor	ration),	1-100	
Further documents are listed in the continuation of Box C	See patent family annex.		
** Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed Date of the actual completion of the international search "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art document member of the same patent family Date of the actual completion of the international search Date of mailing of the international search report			
06 July, 2001 (06.07.01) 17 July, 2001 (17.07.01)			
Name and mailing address of the ISA/ Japanese Patent Office Telephone No.			



Internal application No.
PCT/JP01/03004

Box I Observations where certain claims were found unsearchable (Continuation of item I of first sheet)			
This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:			
1. Claims Nos.: because they relate to subject matter not required to be searched by this Authority, namely:			
2. Claims Nos.: because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:			
3. Claims Nos.: because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).			
Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)			
This International Searching Authority found multiple inventions in this international application, as follows:			
The inventions of the claims of the present international application are divided into the following six groups.			
 The inventions of claims 1-13, 38-51, 77, 83 The inventions of claims 14-30, 52-69, 78-82, 84-88 The inventions of claims 31-37, 70-76 The inventions of claims 89, 90 The inventions of claims 91-96 The inventions of claims 97-100 			
1. As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.			
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.			
3. As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:			
4. No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:			
Remark on Protest The additional search fees were accompanied by the applicant's protest.			
No protest accompanied the payment of additional search fees.			

		1/03004
C(続き).	関連すると認められる文献	
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-250571 A(松下電器産業株式会社) 17.9月.1999(17.09.99),全頁を参照(ファミリーなし)	1-100
A	JP 11-250570 A(松下電器産業株式会社) 17.9月.1999(17.09.99),第13欄第17行-第16欄第32行(ファミリーなし)	1-100
Α	JP 11-126425 A (ソニー株式会社) 11.5月.1999(11.05.99),全頁を参照(ファミリーなし)	1-100
A	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9. 7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
Α	WALDVOGEL, M. et al. The VersaKey Framework: Versatile Group Key Management. IEEE Journal on Selected Areas in Communications. Septemper 1999, Vol. 17, No. 9, p. 1614-1631, especially pp. 1616-1621	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
A	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98, 1998, p. 68-79 especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
A	5C Digital Transmission Content Protection White Paper. Revision 1.0, 1998, p.3, 11, 12 (http://www.dtcp.com)	1-100
PA	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-100
	·	
·		
	·	

. `., ...

発明の属する分野の分類(国際特許分類(IPC))

Int. Cl' H04L9/00, G11B20/10, G11B20/12

調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. Cl' H04L9/00, G11B20/10, G11B20/12, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報

1922-1996年

日本国公開実用新案公報

1971-2001年

日本国登録実用新案公報

1994-2001年

日本国実用新案登録公報

1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, JICST科学技術文献データベース key, tree, generation, DVD

	一 (田油・):	スト製みたわずかれ		
		すると認められる文献		
	引用文献の			
	カテゴリー*	引用文献名 及其一如《统元》即来上来,上,	関連する	
		引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	請求の範囲の番号	
	X	JP 10-3256 A (ソニー株式会社)		
		6.1月.1998(06.01.98),第37-48段落 (ファミリーなし)	89, 90	
	A	3.171.1330(00.01.50),第37-48段格(ファミリーなし)		
	1 4		1-88, 91-100	
	1		1 00, 91-100	
	A	JP 11-39795 A (株式会社東芝)	4 444	
	-	12.2月.1999(12.02.99), 全頁を参照 &	1-100	
		KR 99013756 A & CN 1208925 A		
		Mr. 22019130 V & CM 1509529 V		
	1 . 1	TD 10 00000	Ī	
i	A	JP 10-293726 A (株式会社東芝)	1 100	
	1 1	4.11月.1998(04.11.98),全頁を参照 (ファミリーなし)	1-100	
	1 1	一 一		

区 C欄の続きにも文献が列挙されている。

□ パテントファミリーに関する別紙を参照。

引用文献のカテゴリー

- 「A」特に関連のある文献ではなく、一般的技術水準を示す もの
- 「E」国際出願日前の出願または特許であるが、国際出願日 以後に公表されたもの
- 「L」優先権主張に疑義を提起する文献又は他の文献の発行 日若しくは他の特別な理由を確立するために引用する 文献 (理由を付す)
- 「O」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

- の日の後に公表された文献
- 「T」国際出願日又は優先日後に公表された文献であって 出願と矛盾するものではなく、発明の原理又は理論 の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明 の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以 上の文献との、当業者にとって自明である組合せに よって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

国際調査を完了した日

06.07.01

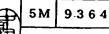
国際調査報告の発送日

17.07.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP).

郵便番号100-8915 東京都千代田区霞が関三丁目4番3号 特許庁審査官 (権限のある職員) 中里 裕正



電話番号 03-3581-1101 内線 3597

国際調査報告

国際出願番号 PCT/JP01/03004

第1欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)
法第8条第3項 (PCT17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。
1. □ 請求の範囲は、この国際調査機関が調査をすることを要しない対象に係るものである。 つまり、
2. 計求の範囲 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. 計求の範囲 は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に 従って記載されていない。
第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)
次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。
この出願の発明は、下記の6群の発明に区分される。
1. 請求の範囲 1-13,38-51,77,83 2. 請求の範囲14-30,52-69,78-82,84-88 3. 請求の範囲31-37,70-76 4. 請求の範囲89,90 5. 請求の範囲91-96 6. 請求の範囲97-100
1. X 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3.
4. 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。
追加調査手数料の異議の申立てに関する注意 □ 追加調査・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
□ 追加調査手数料の納付と共に出願人から異議申立てがあった。図 追加調査手数料の納付と共に出願人から異議申立てがなかった。

SK01PCT44 PCT 0 6. 4. 0 1 受領印

0-1	国際出願番号.	06.4.01)
0-2	国際出願日	受領印
0-3	(受付印)	
0-4	 様式-PCT/RO/101 この特許協力条約に基づく国際	
0-4-1	出願願書は、 右記によって作成された。	PCT-EASY Version 2.91 (updated 01.01.2001)
0-5	申立て 出願人は、この国際出願が特許 協力条約に従って処理されるこ とを請求する。	
0-6	出願人によって指定された受理 官庁	日本国特許庁(RO/JP)
0-7	出願人又は代理人の書類記号	SK01PCT44
ī	発明の名称	情報記録装置、情報再生装置、情報記録方法、情報再 生方法
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
I I -2	右の指定国についての出願人で ある。	米国を除くすべての指定国 (all designated States except US)
II-4ja	名称	リソニー株式会社
II-4en	Name	SONY CORPORATION
II-5 ja	あて名:	141-0001 日本国
II-5en	Address:	東京都 品川区 北品川6丁目7番35号 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
II-6	国籍 (国名)	日本国 JP
11-7	住所(国名)	日本国 JP
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である(applicant and inventor)
III-1-2	右の指定国についての出願人である。	米国のみ (US only)
III-1-4ja	氏名(姓名)	浅野 智之
III-1-4en	Name (LAST, First)	ASANO, Tomoyuki
III-1-5ja	あて名:	141-0001 日本国
III-1-5en	Address:	東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-1-6	国籍 (国名)	日本国 JP
111-1-7	住所(国名)	日本国 JP
	·	

111-2	その他の出願人又は発明者	
III-2-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-2-2	右の指定国についての出願人で	
III-2-4ja	ある。 氏名(姓名)	大澤 義知
	Name (LAST, First)	OSAWA, Yoshitomo
	あて名:	141-0001 日本国
	Address:	東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
111-2-6	国籍(国名)	日本国 JP
111-2-7	住所(国名)	日本国 JP
111-3	その他の出願人又は発明者	
III-3-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
111-3-2	右の指定国についての出願人で ある。	米国のみ (US only)
	氏名(姓名)	石黒 隆二
	Name (LAST, First)	ISHIGURO, Ryuji
III-3-5ja	あて名:	141-0001 日本国
111-3-6	Address: 国籍(国名)	東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP
III-3-7	住所(国名)	日本国 JP
III-4 III-4-1	その他の出願人又は発明者	ILLES Trackers to Z (configuration)
III-4-1 III-4-2	この欄に記載した者は 右の指定国についての出願人で	出願人及び発明者である (applicant and inventor)
	ある。	
	氏名(姓名)	光澤 敦
	Name (LAST, First)	MITSUZAWA, Atsushi
111-4-5ja	あて名:	141-0001 日本国
111-4-5en	Address:	東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
111-4-6	 国籍(国名)	日本国 JP
111-4-7	住所(国名)	日本国 JP
		ure v

III-6-1	VIV 2	The second secon	
III-5-2			
III-5-4ia 氏名(姓名) 大石 文於 OISHI, Tateo 141-0001 日本国 東京都 品川区 北品川 6 T目 7番 3 5号 ソニー株式会社内 C/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本日 JP 日本国 JP			出願人及び発明者である (applicant and inventor)
III-5-4ja Name (LAST, First)	III-5-2		米国のみ (US only)
III-5-5en	III-5-4ja	氏名(姓名)	大石 寸於
141-0001 日本国東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 c o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本国 東京都 品川区 北島川 6 丁目 7 番 3 5 号 ソニー株式会社内 c o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本日 JP			
東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 (/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本日 日本日 JP 日本日 日本日 日本日 JP 日本日 日本日 日本日 JP	III-5-5 ia	セッタ:	
V = 一株式会社内	111 0 034	あく右:	東京都 品川区
III-6-6 国籍 (国名)	III-5-5en	Address:	ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001
III-6-7 住所 (国名)	111-5-6	団体 (団々)	
111-6-1			
コロー6-1 コロー6-2 コロータ コロータ コロータ コロータ コロータ コロータ コロータ コロータ			<u>日本国 JP </u>
Hil-6-2		その他の出願人又は発明者	
ある。 氏名(姓名) Name (LAST, First) あて名: III-6-5ia III-6-5ia Address: Address: Address: Address: Address: III-6-6 III-6-7 III-6-8 III-6-7 III-6-8 III-6-7 III-6-8 III-6-7 III-6-8 III-6-7 III-6-8 III-6-7 III-6-8 III-6-8 III-6-9 III-6-9 III-6-9 III-6-1 III-6-1 III-6-1 III-6-1 III-6-1 III-6-2 III-6-2 III-6-3 III-6-3 III-6-4 III-6-5 III-6-5 III-6-5 III-6-5 III-6-6 III-6-7 III-6-6 III-6-7 III-6-6 III-6-7 III-6-6 III-6-7 III-6-8 III-6-8 III-6-9 I			
III-6-4ja 氏名(姓名) Rame (LAST, First) Rame (LAST, First) 表で名:	111-6-2		米国のみ (US only)
III-6-4en Name (LAST, First) TAKI, Ryuta 141-0001 日本国東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 C/O SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本国	III-6-4ja		瀧 降太
111-6-5ija あて名:			
東京都 品川区 北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本国 JP 日本国 JP 日本国 JP 「代理人又は共通の代表者、通知 のあて名 下記の者は国際機関において右 記のごとく出願人のために行動 する。 氏名(姓名) IV-1-1ja に名(姓名) IV-1-2ja あて名: IV-1-2ja あて名: IV-1-2ia Name (LAST, First) あて名: IV-1-2en Address: 「ROUTE Address: IV-1-2en Name (LAST, First) Name (LAST, First) No.11 Mori Bldg., 6-4, Toranomon 2-chome Minato-ku, Tokyo 105-0001 Japan 03-3508-8266			
III-6-6 国籍 (国名) 日本国 JP	III-6-5en	Address:	北品川6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001
IV-1 住所 (国名) 日本国 JP 代理人又は共通の代表者、通知 のあて名 下記の者は国際機関において右 記のごとく出願人のために行動 する。 氏名(姓名) K名(姓名) Name (LAST, First) あて名:	111-6-6	国籍 (国名)	
Page			
Tillo Till	17 1	1V圧人人は六週の1V攻白、週別 のおイタ	
V-1-1ja K名(姓名) Name (LAST, First) Name (LAST, First) あて名:		下記の者は国際機関において右記のごとく出願人のために行動	代理人(agent)
IV-1-len IV-1-2ja Name (LAST, First) KOIKE, Akira 105-0001 日本国東京都 港区東京都 港区	IV-1-1ja		小池 晃
IV-1-2ja あて名: 105-0001 日本国東京都 港区東京都 港区 虎ノ門二丁目 6 番 4 号 第 1 1 森ピル			
東京都 港区 虎ノ門二丁目 6 番 4 号 第 1 1 森ビル No.11 Mori Bldg., 6-4, Toranomon 2-chome Minato-ku, Tokyo 105-0001 Japan 03-3508-8266		· · · · · · · · · · · · · · · · · · ·	
Ⅳ-1-3 電話番号			東京都 港区 虎ノ門二丁目6番4号 第11森ビル No.11 Mori Bldg., 6-4, Toranomon 2-chome Minato-ku, Tokyo 105-0001
	IV-1-2	康红亚 里	
	14-1-4	ファクンミリ番号	03-3508-0439

	町本 中町口川 2001年04万00日 (00.01.1800.7) 並に出 10.01.27 10.0			
IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additiona)		
		agent(s) with same address as first named agent)		
IV-2-1ja	氏名	田村 榮一; 伊賀 誠司		
IV-2-1en	Name(s)	TAMURA, Eiichi; IGA, Seiji		
V	国の指定	174101011; 2471; 301]		
V-1	広域特許	AP: GH GM KE LS MW MZ SD SL SZ TZ UG ZW		
	(他の種類の保護又は取扱いを	及びハラレプロトコルと特許協力条約の締約国である		
	求める場合には括弧内に記載す	他の国		
	る。)	EA: AM AZ BY KG KZ MD RU TJ TM		
		及びユーラシア特許条約と特許協力条約の締約国で		
		ある他の国		
		EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU		
		MC NL PT SE TR		
		及びヨーロッパ特許条約と特許協力条約の締約国で		
		ある他の国		
		OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG		
		及びアフリカ知的所有権機構と特許協力条約の締約国		
		である他の国		
V-2	国内特許	AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH&LI		
	(他の種類の保護又は取扱いを 求める場合には括弧内に記載す	CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM		
	3。)	HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT		
		LO LY INCOME INCOME INCOME INCOME INCOME		
	,	OD OL OU OI ON OL IO III IN II IL ON OO OO OL		
V-5		YU ZA ZW		
∀ −5	指定の確認の宣言 出願人は、上記の指定に加えて			
	、規則4.9(b)の規定に基づき、			
	特許協力条約のもとで認められ	·		
	る他の全ての国の指定を行う。			
	ただし、V-6欄に示した国の指 定を除く。出願人は、これらの			
	追加される指定が確認を条件と			
	していること、並びに優先日か			
	ら15月が経過する前にその確認			
	がなされない指定は、この期間			
	の経過時に、出願人によって取 り下げられたものとみなされる			
	ことを宣言する。			
V-6	指定の確認から除かれる国	なし(NONE)		
VI-1	先の国内出願に基づく優先権主 張			
*** * *	以	0000 (00 04 0000)		
VI-1-1	先の出願日	2000年04月06日(06.04.2000)		
VI-1-2	先の出願番号	特願2000-105328		
VI-1-3	国名	日本国 JP		
VI-2	先の国内出願に基づく優先権主			
VI-2-1	張 先の出願日	2000年04月07日(07.04.2000)		
VI-2-2	元の山願日 先の出願番号	特願2000-106039		
VI -2-3	元の丘願番号 国名	 		
77 2 0	凹位	ロ4日 パ		

VI-3	[北京日本山田)-廿37周北佐子		
V1-3	先の国内出願に基づく優先権主 張		
VI-3-1	100 先の出願日	2000年06月07日(07.06.20	000)
VI-3-2	先の出願番号	特願2000-170604	•
VI-3-3	国名	日本国 JP	
VI-4	先の国内出願に基づく優先権主		-
VI-4-1	張	0000 / 10 05 12 26	100)
VI 4 1	先の出願日 先の出願番号	2000年12月25日(25.12.20 特願2000-391976)00 <i>)</i>
VI-4-3	元の山殿番号 国名	行願	
VII-1	国石 特定された国際調査機関(ISA)	日本国特許庁(ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	6	-
V111-2	明細書	70	-
A111-3	請求の範囲	23	-
VIII-4	要約	1	absk01pct44.txt
VIII-5	図面	37	-
VIII-7	合計	137	
	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-9	別個の記名押印された委任状	✓	
VIII-10	包括委任状の写し	*	_
VIII-12	優先権証明書	優先権証明書 VI-1,	-
VIII-16	PCT-EASYディスク	VI-2, VI-3, VI-4	フレキシブルディスク
VIII-17	その他	納付する手数料に相当す	-
		る特許印紙を貼付した書面	
VIII-17	その他	国際事務局の口座への振 込を証明する書面	-
VIII-18	要約書とともに提示する図の番号	14	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX-1	提出者の記名押印		
IX-1-1	氏名(姓名)	 小池 晃	
1X-2	提出者の記名押印	, , , , , , , , , , , , , , , , , , , ,	
IX-2-1	氏名(姓名)	 田村 榮一	
IX-3	提出者の記名押印	HIIJ 7K	
IX-3-1	 氏名(姓名)	伊賀 誠司	
		受理官庁記入欄	
10-1	Enther (1881).		
	国際出願として提出された書類 の実際の受理の日		
10-2	図面:		
10-2-1 10-2-2	受理された 不足図面がある		
10 2 2	「一下区国でのの	L	

特許協定	力条約に基づく国際出願願書 副本 - 印刷日時 20	001年04月06日 (06.04.2001) 金曜日 15時21分10秒	2K01PC144
10-3	国際出願として提出された書類 を補完する書類又は図面であっ てその後期間内に提出されたも のの実際の受理の日(訂正日)		
10-4	特許協力条約第11条(2)に基づ く必要な補完の期間内の受理の 日		
10-5	出願人により特定された国際調 査機関	ISA/JP	
10-6	調査手数料未払いにつき、国際 調査機関に調査用写しを送付し ていない		
		国際事務局記入欄	
11-1	記録原本の受理の日		

EP · US

PCI



国際調査報告

(法8条、法施行規則第40、41条) [PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 SK01PCT44		奈調査報告の送付: び下記5を参照す	通知様式(PCT/ISA/220) ること。
国際出願番号 PCT/JP01/03004	国際出願日 (日.月.年) 06.04.	優先日 (日.月.	年) 06.04.00
出願人 (氏名又は名称) ソニー株式	会社 		•
国際調査機関が作成したこの国際調査この写しは国際事務局にも送付される		 CT18条) の規	定に従い出願人に送付する。
この国際調査報告は、全部で4	ページである。		
この調査報告に引用された先行打	術文献の写しも添付されてい	5.	
1. 国際調査報告の基礎 a. 言語は、下記に示す場合を除く この国際調査機関に提出さ			
b. この国際出願は、ヌクレオチト この国際出願に含まれる書	面による配列表		基づき国際調査を行った。
	れたフレキシブルディスクによ 関に提出された書面による配列		
	関に提出されたフレキシブルデ	•	表
□ 出願後に提出した書面によ 書の提出があった。	5配列表が出願時における国際	出願の開示の範囲]を超える事項を含まない旨の陳述
	こ配列とフレキシブルディスク	による配列表に記	2録した配列が同一である旨の陳述
2. 請求の範囲の一部の調査が	できない(第I欄参照)。		
3. 区 発明の単一性が欠如してい	る(第Ⅱ欄参照)。		
4. 発明の名称は	i人が提出したものを承認する。	· -	• •
区 次に	示すように国際調査機関が作品	戈した。	. ••
_	情報記録/再生	装置及び方法	
5. 要約は 🗵 出願	人が提出したものを承認する。	•	
国際		は、この国際調査	P C T 規則38.2(b)) の規定により 報告の発送の日から1カ月以内にこ
6. 要約書とともに公表される図は、 第 <u>14</u> 図とする。X 出願	[人が示したとおりである。		□ なし
□ 出額	i人は図を示さなかった。		
	は発明の特徴を一層よく表し	でいる。 	

第1個 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)
法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。
1. 請求の範囲 は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. 請求の範囲 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. □ 請求の範囲は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に
従って記載されていない。
第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)
次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。
この出願の発明は、下記の6群の発明に区分される。
1. 請求の範囲 1-13,38-51,77,83 2. 請求の範囲14-30,52-69,78-82,84-88 3. 請求の範囲31-37,70-76 4. 請求の範囲89,90
4. 請求の範囲95,90 5. 請求の範囲91-96 6. 請求の範囲97-100
1. X 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求 の範囲について作成した。
2. □ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. □ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。
追加調査手数料の異議の申立てに関する注意 □ 追加調査手数料の納付と共に出願人から異議申立てがあった。
図 追加調査手数料の納付と共に出願人から異議申立てがなかった。

Α.	発明の属する分野の分類	(国際特許分類((IPC)	•)	,
----	-------------	----------	-------	-----	---

Int. Cl' H04L9/00, G11B20/10, G11B20/12

B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. Cl' H04L9/00, G11B20/10, G11B20/12, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報

1922-1996年

日本国公開実用新案公報

1971-2001年

日本国登録実用新案公報

1994-2001年

日本国実用新案登録公報

1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, JICST科学技術文献データベース key, tree, generation, DVD

C. 関連すると認められる文献

0. 122.7	D C HOUND STATE OF THE STATE OF	
引用文献の		関連する
カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	請求の範囲の番号
: X	JP 10-3256 A (ソニー株式会社) - 6.1月.1998(06.01.98), 第37-48段落 (ファミリーなし)	89, 90
A	0.177.1000 (00.01.00), MOL 101XIII (7717 & 07	1-88, 91-100
Α .	JP 11-39795 A (株式会社東芝) 12.2月.1999(12.02.99),全頁を参照 & KR 99013756 A & CN 1208925 A	1-100
A	JP 10-293726 A (株式会社東芝) 4.11月.1998(04.11.98),全頁を参照(ファミリーなし)	1-100

X C欄の続きにも文献が列挙されている。

□ パテントファミリーに関する別紙を参照。

- * 引用文献のカテゴリー
- 「A」特に関連のある文献ではなく、一般的技術水準を示す
- 「E」国際出願日前の出願または特許であるが、国際出願日 以後に公表されたもの
- 「L」優先権主張に疑義を提起する文献又は他の文献の発行 日若しくは他の特別な理由を確立するために引用する 文献(理由を付す)
- 「O」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」国際出願日又は優先日後に公表された文献であって 出願と矛盾するものではなく、発明の原理又は理論 の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明 の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以 上の文献との、当業者にとって自明である組合せに よって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

国際調査を完了した日

06.07.01

国際調査報告の発送日

17.07.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP) 郵便番号100-8915

郵便番号100-8915 東京都千代田区霞が関三丁目4番3号 特許庁審査官(権限のある職員) 中里 裕正



9364

電話番号 03-3581-1101 内線 3597

		国际网 直	国际山願番	1/03004	
	C (続き).				
	引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは	、その関連する箇所の表示	関連する 請求の範囲の番号	
	Α .	JP 11-250571 A (松下電器産業株式会社) 17.9月.1999(17.09.99),全頁を参照(ファミ		1-100	
	· A	JP 11-250570 A (松下電器産業株式会社) 17.9月.1999(17.09.99),第13欄第17行-第	16欄第32行(ファミリーなし)	1-100	
	A	JP 11-126425 A (ソニー株式会社) 11.5月.1999(11.05.99), 全頁を参照 (ファミ	リーなし)	1–100	
	Α	JP 11-187013 A (日本アイ・ビー・エム株 9. 7月.1999(09.07.99) 第9-11, 17-22段 & CN 1224962 A	式会社) 落	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100	
	A	WALDVOGEL, M. et al. The VersaKey Framework: Versatile Group IEEE Journal on Selected Areas in Common Septemper 1999, Vol. 17, No. 9, p. 1614-16 especially pp. 1616-1621	unications.	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100	
	A	WONG, C.K. et al. Secure Group Communications Using Key (Proceedings of ACM SIGCOMM'98, 1998, p. especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/	68-79	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100	
	Α	5C Digital Transmission Content Protect Revision 1.0, 1998, p.3, 11, 12 (http://www.dtcp.com)	tion White Paper.	1-100	
	PA	館林誠 他,記録メディアのコンテンツ保護 2000年電子情報通信学会基礎・境界ソサイ 7.9月.2000(07.09.00), p.367-368	システム, エティ大会講演論文集,	1-100	
				·	
İ					
			,		
L					